

IPSP Working Group
Internet Draft
[draft-ietf-ipsec-conf-mib-04.txt](#)

M. Baer
Network Associates Inc
R. Charlet
W. Hardaker
Network Associates Inc
R. Story
Revelstone Software
C. Wang
Smartpipes Inc
Jul 2002

IPsec Policy Configuration MIB
draft-ietf-ipsec-conf-mib-04.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#). Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

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

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

1. Introduction

This document defines a configuration MIB for IPsec [[IPSEC](#)]/IKE [[IKE](#)] policy. It does not define MIBs for monitoring the state of an IPsec device. It does not define MIBs for configuring other policy related actions. The purpose of this MIB is to allow administrators to be able to configure policy with respect to the IPsec/IKE protocols. However, some of the packet filtering and matching of conditions to actions is of a more general nature than IPsec only.

It is possible to add other packet transforming actions to this MIB if those actions needed to be performed conditionally on filtered traffic.

2. The SNMP Management Framework

The SNMP Management Framework presently consists of five major components:

- o An overall architecture, described in [RFC 2571](#) [[SNMPARCH](#)].
- o Mechanisms for describing and naming objects and events for the purpose of management. The first version of this Structure of Management Information (SMI) is called SMIV1 and described in STD 16, [RFC 1155](#) [[SMIV1](#)], STD 16, [RFC 1212](#) [[MIB](#)] and [RFC 1215](#) [[TRAPS](#)]. The second version, called SMIV2, is described in STD 58, [RFC 2578](#) [[SMIV2](#)], [RFC 2579](#) [[SNMPTC](#)] and [RFC 2580](#) [[SNMPCONF](#)].
- o Message protocols for transferring management information. The first version of the SNMP message protocol is called SNMPv1 and described in STD 15, [RFC 1157](#) [[SNMPv1](#)]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in [RFC 1901](#) [[SNMPv2c](#)] and [RFC 1906](#) [[SNMPv2TM](#)]. The third version of the message protocol is called SNMPv3 and described in [RFC 1906](#) [[snmpv2TM](#)], [RFC 2572](#) [[SNMPv3](#)] and [RFC 2574](#) [[SNMPUSM](#)].
- o Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is described in STD 15, [RFC 1157](#) [[SNMPv1](#)]. A second set of protocol operations and associated PDU formats is described in [RFC 1905](#) [[SNMPv2](#)].
- o A set of fundamental applications described in [RFC 2573](#) [[SNMPAPP](#)] and the view-based access control mechanism described in [RFC 2575](#) [[SNMPVACM](#)].

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

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

defined using the mechanisms defined in the SMI.

This memo specifies a MIB module that is compliant to the SMIV2. A MIB conforming to the SMIV1 can be produced through the appropriate translations. The resulting translated MIB must be semantically

equivalent, except where objects or events are omitted because no translation is possible (use of Counter64). Some machine readable information in SMIV2 will be converted into textual descriptions in SMIV1 during the translation process. However, this loss of machine readable information is not considered to change the semantics of the MIB.

3. Relationship to the DMTF Policy Model

The Distributed Management Task Force has created an object oriented model of IPsec policy information known as the IPsec Policy Model White Paper [[IPSECPM](#)]. The contents of this document are also reflected in the internet draft "IPsec Configuration Policy Model" (IPCP) [[IPCP](#)]. This MIB is a task specific derivation of the IPCP for use with SNMPv3.

A detailed comparison between this MIB and the IPSP model can be found in [Appendix A](#). However, the high-level areas where this MIB diverges from the IPCP model are:

- o Policies, Groups, Conditions, and some levels of Action are generically named. That is we dropped prefixes like "SA", or "ipsec". This is because we feel that packet classification and matching of conditions to actions is more general than IPsec and could possibly be reused by other packet transforming actions which need to conditionally act on packets matching filters.
- o Filters are implemented in a more generic and scalable manner, rather than enforcing the condition/filtering pairing and their restrictions upon the user. The MIB offers a compound filter object to provide for greater flexibility when creating complex filters.

[4.](#) Definitions

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

```
IMPORTS
```

```
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, Integer32,  
    Unsigned32, experimental FROM SNMPv2-SMI
```

```
    TEXTUAL-CONVENTION, RowStatus, TruthValue,  
    TimeStamp, StorageType, VariablePointer, DateAndTime  
    FROM SNMPv2-TC
```

```
    MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP  
    FROM SNMPv2-CONF
```

```
    SnmpAdminString FROM SNMP-FRAMEWORK-MIB
```

```
    IkeHashAlgorithm, IpsecDoiEncapsulationMode,  
    IpsecDoiIpcompTransform,  
    IpsecDoiAuthAlgorithm, IpsecDoiEspTransform,  
    IpsecDoiSecProtocolId,  
    IkeGroupDescription, IpsecDoiIdentType,  
    IkeEncryptionAlgorithm, IkeAuthMethod FROM IPSEC-ISAKMP-IKE-DOI-TC;
```

```
--
```

```
-- module identity
```

```
--
```

ipsecPolicyMIB MODULE-IDENTITY

LAST-UPDATED "200102230000Z" -- 23 February 2001

ORGANIZATION "IETF IP Security Policy Working Group"

CONTACT-INFO "Michael Baer

Network Associates, Inc.
3965 Freedom Circle, Suite 500
Santa Clara, CA 95054
Phone: +1 530 304 1628
Email: mike_baer@nai.com

Ricky Charlet
Email: rcharlet@alumni.calpoly.edu

Wes Hardaker
Network Associates, Inc.
3965 Freedom Circle, Suite 500
Santa Clara, CA 95054
Phone: +1 530 400 2774
Email: wes_hardaker@nai.com

Various Authors

[Page 4]

Internet Draft

IPsec Policy Configuration MIB

June 2002

Robert Story
Revelstone Software
PO Box 1474
Duluth, GA 30096
Phone: +1 770 617 3722
Email: ipsp-mib@revelstone.com

Cliff Wang
SmartPipes Inc.
Suite 300, 565 Metro Place South
Dublin, OH 43017
Phone: +1 614 923 6241
E-Mail: CWang@smartpipes.com"

DESCRIPTION

"The MIB module for defining IPsec Policy filters and actions"

-- Revision History

REVISION "200111210000Z"

-- 21 November 2001

DESCRIPTION "Many updates and restructuring to match changes in the ipsp policy model."

REVISION "200107200000Z" -- 20 July 2001
DESCRIPTION "Many updates and restructuring to match changes in
the ipsp policy model."

REVISION "200102230000Z" -- 23 February 2001
DESCRIPTION "This is the initial version of this MIB."

::= { mib-2 XXX }

--
-- groups of related objects
--

ipsecPolicyConfigObjects OBJECT IDENTIFIER ::= { ipsecPolicyMIB 1 }
ipsecPolicyNotificationObjects OBJECT IDENTIFIER ::= { ipsecPolicyMIB 2 }
ipsecPolicyConformanceObjects OBJECT IDENTIFIER ::= { ipsecPolicyMIB 3 }

--
-- Textual Conventions
--

IpssecBooleanOperator ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"The IpssecBooleanOperator operator is used to specify whether
sub-components in a decision making process are ANDed or ORed

Various Authors

[Page 5]

Internet Draft

IPsec Policy Configuration MIB

June 2002

together to decide if the resulting expression is true or false."
SYNTAX INTEGER { or(0), and(1) }

IpssecIsNegated ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"The IpssecIsNegated operator is used to specify whether
or not the results of a sub-component's return clause is taken
as is, or if the logical negation of the result is used instead."

SYNTAX INTEGER { no(0), yes(1) }

IpssecSADirection ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"The IpssecSADirection operator is used to specify whether

or not a row should apply to outgoing or incoming SAs."
SYNTAX INTEGER { outgoing(0), incoming(1) }

IpssecIPVersion ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"Valid values for Internet Protocol versions handled by the
IPsec policy system."

SYNTAX INTEGER { unknown(0), ipv4(4), ipv6(6) }

IpssecIPAddress ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"An IpssecIPAddress is an IPv4 or IPv6 IP address, in network
byte order."

SYNTAX OCTET STRING (SIZE(4|16|20))

--

-- Policy group definitions

--

ipsecLocalConfigObjects OBJECT IDENTIFIER ::= { ipsecPolicyConfigObjects 1 }

systemPolicyGroupName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(0..32))

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This object indicates the policy group containing the global
system policy that is to be applied when a given endpoint
does not contain a policy definition. Its value can be used
as an index into the policyGroupContentsTable to retrieve a
list of policies. A zero length string indicates no system

wide policy exists and the default policy of 'accept' should be
executed until one is imposed by either this object or by the
endpoint processing a given packet."

::= { ipsecLocalConfigObjects 1 }

policyEndpointToGroupTable OBJECT-TYPE

SYNTAX SEQUENCE OF PolicyEndpointToGroupEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This table is used to map policy (groupings) onto an endpoint where traffic is to pass by. Any policy group assigned to an endpoint is then used to control access to the traffic passing by it.

If an endpoint has been configured with a policy group and no contained rule matches the incoming packet, the default action in this case shall be to drop the packet.

If no policy group has been assigned to an endpoint, then the policy group specified by systemPolicyGroupName should be used for the endpoint."

::= { ipsecPolicyConfigObjects 2 }

policyEndpointToGroupEntry OBJECT-TYPE

SYNTAX PolicyEndpointToGroupEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A mapping assigning a policy group to an endpoint."

INDEX { peEndpointIdentType, peEndpointAddress }

::= { policyEndpointToGroupTable 1 }

PolicyEndpointToGroupEntry ::= SEQUENCE {

peEndpointIdentType

IpsecIPVersion,

peEndpointAddress

IpsecIPAddress,

peGroupName

SnmpAdminString,

peLastChanged

TimeStamp,

peStorageType

StorageType,

peRowStatus

RowStatus

}

peEndpointIdentType OBJECT-TYPE

SYNTAX IpsecIPVersion

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The Internet Protocol version of the address associated with

of octets in network byte order. When combined with the peEndpointAddress these objects can be used to uniquely identify an endpoint that a set of policy groups should be applied to. Devices supporting IPv4 MUST support the ipv4 value, and devices supporting IPv6 MUST support the ipv6 value."

::= { policyEndpointToGroupEntry 1 }

peEndpointAddress OBJECT-TYPE

SYNTAX IpsecIPAddress

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The address of a given endpoint, the format of which is specified by the peEndpointIdentType object."

::= { policyEndpointToGroupEntry 2 }

peGroupName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(1..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The policy group name to apply to this endpoint. The value of the peGroupName object should then be used as an index into the policyGroupContentsTable to come up with a list of rules that MUST be applied to this endpoint."

::= { policyEndpointToGroupEntry 3 }

peLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { policyEndpointToGroupEntry 4 }

peStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

```
DEFVAL { nonVolatile }
 ::= { policyEndpointToGroupEntry 5 }
```

```
peRowStatus OBJECT-TYPE
```

```
SYNTAX      RowStatus
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
```

```
"This object indicates the conceptual status of this row.
```

```
The value of this object has no effect on whether other
objects in this conceptual row can be modified.
```

```
This object may not be set to active until one or more active rows
exist within the policyGroupContentsTable for the group referenced
by the peGroupName object."
```

```
 ::= { policyEndpointToGroupEntry 6 }
```

```
--
-- policy group definition table
--
```

```
policyGroupContentsTable OBJECT-TYPE
```

```
SYNTAX      SEQUENCE OF PolicyGroupContentsEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
```

```
"This table contains a list of rules and/or subgroups
contained within a given policy group. The entries are
sorted by the pgcPriority object and MUST be executed in
order according to this value, starting with the lowest
value. Once a group item has been processed, the processor
MUST stop processing this packet if an action was executed as
a result of the processing of a given group. Iterating into
the next policy group item by finding the next largest
pgcPriority object shall only be done if no actions were
run when processing the last item for a given packet."
```

```
 ::= { ipsecPolicyConfigObjects 3 }
```

```
policyGroupContentsEntry OBJECT-TYPE
```

```
SYNTAX      PolicyGroupContentsEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
```

```
"Defines a given sub-item within a policy group."
```

```
INDEX      { pgcName, pgcPriority }
```

```
::= { policyGroupContentsTable 1 }
```

```
PolicyGroupContentsEntry ::= SEQUENCE {  
    pgcName                SnmpAdminString,  
    pgcPriority             Integer32,  
    pgcFilter              VariablePointer,  
    pgcGroupComponentType INTEGER,  
    pgcGroupComponentName SnmpAdminString,  
    pgcLastChanged        TimeStamp,  
    pgcStorageType         StorageType,  
    pgcRowStatus           RowStatus  
}
```

pgcName OBJECT-TYPE

```
SYNTAX      SnmpAdminString (SIZE(1..32))  
MAX-ACCESS  not-accessible  
STATUS      current  
DESCRIPTION  
    "The administrative name of this group."  
 ::= { policyGroupContentsEntry 1 }
```

pgcPriority OBJECT-TYPE

```
SYNTAX      Integer32 (0..65536)  
MAX-ACCESS  not-accessible  
STATUS      current  
DESCRIPTION  
    "The priority (sequence number) of the sub-component in this group."  
 ::= { policyGroupContentsEntry 2 }
```

pgcFilter OBJECT-TYPE

```
SYNTAX      VariablePointer  
MAX-ACCESS  read-create  
STATUS      current  
DESCRIPTION  
    "pgcFilter points to a filter which is evaluated  
    to determine whether the sub-component within this group  
    should be exercised.  Managers can use this object to  
    classify groups of rules or subgroups together in order to  
    achieve a greater degree of control and optimization over the  
    execution order of the items within the group.  If the filter  
    evaluates to false, the rule or subgroup will be skipped and
```

the next rule or subgroup will be evaluated instead.

An example usage of this object would be to limit a group of rules to executing only when the IP packet being process is designated to be processed by IKE. This effecitevly creates a group of IKE specific rules.

This MIB defines the following tables which may be pointed to by this column. Implementations may choose to provide other

filter tables as well:

```
    ipHeaderFilterTable
    timeFilterTable
    compoundFilterTable
    trueFilter
```

If this column is set to a VariablePointer value which references a non-existent row in an otherwise supported table, the inconsistentName exception should be returned. If the table pointed to by the VariablePointer is not supported at all, then an inconsistentValue exception should be returned."

```
DEFVAL { trueFilterInstance }
::= { policyGroupContentsEntry 3 }
```

pgcGroupComponentType OBJECT-TYPE

```
SYNTAX      INTEGER { reserved(0), group(1), rule(2) }
```

```
MAX-ACCESS  read-create
```

```
STATUS      current
```

```
DESCRIPTION
```

```
"Indicates whether the pgcGroupComponentName object is the
name of another group defined within the
policyGroupContentsTable or is the name of a rule defined
within the policyRuleDefinitionTable."
```

```
DEFVAL { rule }
```

```
::= { policyGroupContentsEntry 4 }
```

pgcGroupComponentName OBJECT-TYPE

```
SYNTAX      SnmpAdminString (SIZE(1..32))
```

```
MAX-ACCESS  read-create
```

```
STATUS      current
```

```
DESCRIPTION
```

"The name of the policy rule or subgroup contained within this group, as indicated by the pgcGroupComponentType object."
 ::= { policyGroupContentsEntry 5 }

pgcLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { policyGroupContentsEntry 6 }

pgcStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

Various Authors

[Page 11]

Internet Draft

IPsec Policy Configuration MIB

June 2002

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

DEFVAL { nonVolatile }

::= { policyGroupContentsEntry 7 }

pgcRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other objects in this conceptual row can be modified.

This object may not be set to active until the row to which the pgcGroupComponentName points to exists."

::= { policyGroupContentsEntry 8 }

```

--
-- policy definition table
--

policyRuleDefinitionTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF PolicyRuleDefinitionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table defines a policy rule by associating a filter or a
        set of filters to an action to be executed."
    ::= { ipsecPolicyConfigObjects 4 }

policyRuleDefinitionEntry OBJECT-TYPE
    SYNTAX      PolicyRuleDefinitionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row defining a particular policy definition.  A rule
        definition binds a filter pointer to an action pointer."
    INDEX      { pRuleName }
    ::= { policyRuleDefinitionTable 1 }

```

```

PolicyRuleDefinitionEntry ::= SEQUENCE {
    pRuleName          SnmpAdminString,
    pRuleDescription   OCTET STRING,
    pRuleFilter        VariablePointer,
    pRuleFilterNegated IpsecIsNegated,
    pRuleAction        VariablePointer,
    pRuleAdminStatus   INTEGER,
    pRuleLastChanged   TimeStamp,
    pRuleStorageType   StorageType,
    pRuleRowStatus     RowStatus
}

```

```

pRuleName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "pRuleName is the administratively assigned name of the rule

```

referred to by the pgcGroupComponentName object."
 ::= { policyRuleDefinitionEntry 1 }

pRuleDescription OBJECT-TYPE

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

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"A user definable string. This field may be used for your administrative tracking purposes."

DEFVAL { "" }

::= { policyRuleDefinitionEntry 2 }

pRuleFilter OBJECT-TYPE

SYNTAX VariablePointer

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"pRuleFilter points to a filter which is used to evaluate whether the action associated with this row should be fired or not. The action will only fire if the filter referenced by this object evaluates to TRUE after first applying any negation required by the pRuleFilterNegated object.

This MIB defines the following tables which may be pointed to by this column. Implementations may choose to provide other filter tables as well:

ipHeaderFilterTable

timeFilterTable

Various Authors

[Page 13]

Internet Draft

IPsec Policy Configuration MIB

June 2002

compoundFilterTable

trueFilter

If this column is set to a VariablePointer value which references a non-existent row in an otherwise supported table, the inconsistentName exception should be returned. If the table pointed to by the VariablePointer is not supported at all, then an inconsistentValue exception should be returned."

::= { policyRuleDefinitionEntry 3 }

pRuleFilterNegated OBJECT-TYPE

SYNTAX IpsecIsNegated
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"pRuleFilterNegated specifies whether the filter referenced by
the pRuleFilter object should be negated or not."
DEFVAL { no }
 ::= { policyRuleDefinitionEntry 4 }

pRuleAction OBJECT-TYPE

SYNTAX VariablePointer
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This column points to the action to be taken. It may, but is
not limited to, point to a row in one of the following
tables:

compoundActionsTable
saPreconfiguredActionTable
ikeActionTable
ipsecActionTable

It may also point to one of the scalar objects beneath
saStaticActions.

If this object is set to a pointer to a row in an unsupported
(or unknown) table, an inconsistentValue error should be
returned.

If this object is set to point to a non-existent row in an
otherwise supported table, an inconsistentName error should
be returned."

::= { policyRuleDefinitionEntry 5 }

pRuleAdminStatus OBJECT-TYPE

SYNTAX INTEGER { enabled(1), disabled(2) }

MAX-ACCESS read-create
STATUS current
DESCRIPTION

"Indicates whether the current rule definition should be

considered active. If enabled, it should be evaluated when processing packets. If disabled, packets should continue to be processed by the rest of the rules defined in the policyGroupContentsTable as if this rule's filters had effectively failed."

DEFVAL { enabled }
::= { policyRuleDefinitionEntry 6 }

pRuleLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { policyRuleDefinitionEntry 7 }

pRuleStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

DEFVAL { nonVolatile }
::= { policyRuleDefinitionEntry 8 }

pRuleRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other objects in this conceptual row can be modified.

This object may not be set to active until the containing conditions, filters and actions have been defined. Once active, it must remain active until no policyGroupContents entries are referencing it."

```
 ::= { policyRuleDefinitionEntry 9 }

--
-- Policy compound filter definition table
--

compoundFilterTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CompoundFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table defining a compound set of filters and their
         associated parameters. A row in this table can either be
         pointed to by a pRuleFilter object or by a ficSubFilter object."
    ::= { ipsecPolicyConfigObjects 5 }

compoundFilterEntry OBJECT-TYPE
    SYNTAX      CompoundFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry in the compoundFilterTable. A filter defined by this
         table is considered to have a TRUE return value if and
         only if:

         cfLogicType is AND and all of the sub-filters associated
         with it, as defined in the filtersInCompoundFilterTable,
         are all true themselves (after applying any required
         negation as defined by the ficFilterIsNegated object).

         cfLogicType is OR and at least one of the sub-filters
         associated with it, as defined in the
         filtersInCompoundFilterTable, is true itself
         (after applying any required negation as defined by the
         ficFilterIsNegated object).

    INDEX      { cfName }
    ::= { compoundFilterTable 1 }

CompoundFilterEntry ::= SEQUENCE {
    cfName                SnmpAdminString,
    cfDescription         OCTET STRING,
    cfLogicType           IpvsecBooleanOperator,
    cfLastChanged         TimeStamp,
    cfStorageType         StorageType,
    cfRowStatus           RowStatus
}
}
```

SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"A user definable string. You may use this field for your
administrative tracking purposes."
 ::= { compoundFilterEntry 1 }

cfDescription OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"A user definable string. You may use this field for your
administrative tracking purposes."
DEFVAL { 'H' }
 ::= { compoundFilterEntry 2 }

cfLogicType OBJECT-TYPE

SYNTAX IpsecBooleanOperator
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"Indicates whether the filters contained within this filter
are functionally ANDed or ORed together."
DEFVAL { and }
 ::= { compoundFilterEntry 3 }

cfLastChanged OBJECT-TYPE

SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or created
either through SNMP SETs or by some other external means."
 ::= { compoundFilterEntry 4 }

cfStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create
STATUS current
DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are, in fact, modifiable is implementation specific."

Various Authors

[Page 17]

Internet Draft

IPsec Policy Configuration MIB

June 2002

DEFVAL { nonVolatile }
::= { compoundFilterEntry 5 }

cfRowStatus OBJECT-TYPE

SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other objects in this conceptual row can be modified.

Once active, it may not have its value changed if any active rows in the policyRuleDefinitionTable are currently pointing at this row."

::= { compoundFilterEntry 6 }

--

-- Policy filters in a cf table

--

filtersInCompoundFilterTable OBJECT-TYPE

SYNTAX SEQUENCE OF FiltersInCompoundFilterEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

"This table defines a list of filters contained within a given compound filter set defined in the compoundFilterTable."

::= { ipsecPolicyConfigObjects 6 }

filtersInCompoundFilterEntry OBJECT-TYPE

SYNTAX FiltersInCompoundFilterEntry

MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "An entry into the list of filters for a given compound filter."
INDEX { cfName, ficPriority }
 ::= { filtersInCompoundFilterTable 1 }

FiltersInCompoundFilterEntry ::= SEQUENCE {
 ficPriority Integer32,
 ficSubfilter VariablePointer,
 ficSubfilterIsNegated IpsecIsNegated,
 ficLastChanged TimeStamp,
 ficStorageType StorageType,
 ficRowStatus RowStatus
}

ficPriority OBJECT-TYPE
SYNTAX Integer32 (0..65536)
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "The priority of a given filter within a condition.
 Implementations MAY choose to follow the ordering indicated by
 the manager that created the rows in order to allow the
 manager to intelligently construct filter lists such that
 faster filters are evaluated first."
 ::= { filtersInCompoundFilterEntry 1 }

ficSubfilter OBJECT-TYPE
SYNTAX VariablePointer
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "The location of the contained filter. The value of this column
 should be a VariablePointer which references the properties for
 the filter to be included in this compound filter. This MIB
 defines the following tables which may be pointed to by this
 column. Implementations may choose to provide other filter
 tables as well:

 ipHeaderFilterTable
 timeFilterTable

compoundFilterTable
trueFilter

If this column is set to a VariablePointer value which references a non-existent row in an otherwise supported table, the inconsistentName exception should be returned. If the table pointed to by the VariablePointer is not supported at all, then an inconsistentValue exception should be returned."

::= { filtersInCompoundFilterEntry 2 }

ficSubfilterIsNegated OBJECT-TYPE

SYNTAX IpsecIsNegated

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Indicates whether the result of applying this subfilter should be negated or not."

DEFVAL { no }

::= { filtersInCompoundFilterEntry 3 }

ficLastChanged OBJECT-TYPE

SYNTAX TimeStamp

Various Authors

[Page 19]

Internet Draft

IPsec Policy Configuration MIB

June 2002

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { filtersInCompoundFilterEntry 4 }

ficStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

DEFVAL { nonVolatile }

::= { filtersInCompoundFilterEntry 5 }

```

ficRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This object indicates the conceptual status of this row.

        The value of this object has no effect on whether other
        objects in this conceptual row can be modified.

        This object can not be made active until the filter
        referenced by the ficSubFilter object is both defined and is
        active.  An attempt to do so will result in an
        inconsistentValue error."
 ::= { filtersInCompoundFilterEntry 6 }

--
-- Static Filters
--

staticFilters OBJECT IDENTIFIER ::= { ipsecPolicyConfigObjects 7 }

trueFilter OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "This scalar indicates a (automatic) true result for a

```

```

        filter. I.e. this is a filter that is always true, useful
        for adding as a default filter for a default action or a
        set of actions."
 ::= { staticFilters 1 }

```

```

trueFilterInstance OBJECT IDENTIFIER ::= { trueFilter 0 }

```

```

ikePhase1Filter OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION

```

```
        "This static filter can be used to test if a packet is
        part of an ike phase-1 negotiation."
 ::= { staticFilters 2 }
```

```
ikePhase2Filter OBJECT-TYPE
```

```
    SYNTAX      Integer32
```

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

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "This static filter can be used to test if a packet is
        part of an ike phase-2 negotiation."
```

```
 ::= { staticFilters 3 }
```

```
--
```

```
-- Policy IPHeader filter definition table
```

```
--
```

```
ipHeaderFilterTable OBJECT-TYPE
```

```
    SYNTAX      SEQUENCE OF IpHeaderFilterEntry
```

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

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "This table contains a list of filter definitions to be used
        within the policyRuleDefinitionTable or the
        filtersInCompoundFilter table."
```

```
 ::= { ipsecPolicyConfigObjects 8 }
```

```
ipHeaderFilterEntry OBJECT-TYPE
```

```
    SYNTAX      IpHeaderFilterEntry
```

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

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "A definition of a particular filter."
```

```
    INDEX      { ihfName }
```

```
 ::= { ipHeaderFilterTable 1 }
```

```
IpHeaderFilterEntry ::= SEQUENCE {
```

```
    ihfName
```

```
    ihfType
```

```
    ihfIPVersion
```

```
    ihfSrcAddressBegin
```

```
        SnmpAdminString,
```

```
        BITS,
```

```
        IpsecIPVersion,
```

```
        IpsecIPAddress,
```



```

ihfSrcAddressEnd          IsecIPAddress,
ihfDstAddressBegin       IsecIPAddress,
ihfDstAddressEnd        IsecIPAddress,
ihfSrcLowPort            Integer32,
ihfSrcHighPort          Integer32,
ihfDstLowPort            Integer32,
ihfDstHighPort          Integer32,
ihfProtocol              Integer32,
ihfIPv6FlowLabel        OCTET STRING,
ihfLastChanged           TimeStamp,
ihfStorageType           StorageType,
ihfRowStatus             RowStatus
}

```

ihfName OBJECT-TYPE

```

SYNTAX      SmpAdminString (SIZE(1..32))
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "The administrative name for this filter."
 ::= { ipHeaderFilterEntry 1 }

```

ihfType OBJECT-TYPE

```

SYNTAX      BITS { sourceAddress(0), destinationAddress(1),
                  sourcePort(2), destinationPort(3),
                  protocol(4), ipv6FlowLabel(5) }
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION

```

"This defines the various tests that are used when evaluating a given filter. The results of each test are ANDed together to produce the result of the entire filter. When processing this filter, it is recommended for efficiency reasons that the filter halt processing the instant any of the specified tests fail.

Once a row is 'active', this object's value may not be changed unless all the appropriate columns needed by the new value to be imposed on this object have been appropriately configured.

The various tests definable in this table are as follows:

sourceAddress:

- Tests if the source address in the packet lies between the ihfSrcAddressBegin and ihfSrcAddressEnd objects. Note that setting these two objects to the same address will limit the search to the exact match of a single address. The format and length of the address objects are defined by the ihfIPVersion column.

A row in this table containing a ihfType object with the sourceAddress object bit but without the ihfIPVersion, ihfSrcAddressBegin and ihfSrcAddressEnd objects set will cause the ihfRowStatus object to return the notReady state.

destinationAddress:

- Tests if the destination address in the packet lies between the ihfDstAddressBegin and ihfDstAddressEnd objects. Note that setting these two objects to the same address will limit the search to the exact match of a single address. The format and length of the address objects are defined by the ihfIPVersion column.

A row in this table containing a ihfType object with the destinationAddress object bit but without the ihfIPVersion, ihfDstAddressBegin and ihfDstAddressEnd objects set will cause the ihfRowStatus object to return the notReady state.

sourcePort:

- Tests if the source port of IP packets using a protocol that uses port numbers (at this time, UDP or TCP) lies between the ihfSrcLowPort and ihfSrcHighPort objects. Note that setting these two objects to the same address will limit the search to the exact match of a single port.

A row in this table containing a ihfType object with the sourcePort object bit but without the ihfSrcLowPort, and ihfSrcHighPort objects set will cause the ihfRowStatus object to return the notReady state.

destinationPort:

- Tests if the source port of IP packets using a protocol that uses port numbers (at this time, UDP or TCP) lies between the ihfDstLowPort and ihfDstHighPort objects. Note that setting these two objects to the same address will limit the search to the exact match of a single port.

A row in this table containing a ihfType object with the

sourcePort object bit but without the ihfDstLowPort, and ihfDstHighPort objects set will cause the ihfRowStatus object to return the notReady state.

protocol:

- Tests to see if the packet being processed is for the given protocol type.

A row in this table containing a ihfType object with the protocol object bit but without the ihfProtocol object set will cause the ihfRowStatus object to return the notReady state.

ipv6FlowLabel:

- Tests to see if the packet being processed contains an ipv6 Flow Label which matches the value in the ipfIPv6FlowLabel object. Setting this bit mandates that for the packet to match the filter, it must be an IPv6 packet.

A row in this table containing a ihfType object with the ipv6FlowLabel object bit but without the ipfIPv6FlowLabel object set will cause the ihfRowStatus object to return the notReady state."

::= { ipHeaderFilterEntry 2 }

ihfIPVersion OBJECT-TYPE

SYNTAX IpsecIPVersion

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The Internet Protocol version the addresses are to match against. The value of this property determines the size and format of the ihfSrcAddressBegin, ihfSrcAddressEnd, ihfDstAddressBegin, and ihfDstAddressEnd objects."

DEFVAL { ipv6 }

::= { ipHeaderFilterEntry 3 }

ihfSrcAddressBegin OBJECT-TYPE

SYNTAX IpsecIPAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The starting address of a source address range that the packet must match against for this filter to be considered TRUE.

This object is only used if sourceAddress is set in ihfType."

::= { ipHeaderFilterEntry 4 }

ihfSrcAddressEnd OBJECT-TYPE

SYNTAX IpsecIPAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The ending address of a source address range to check a packet against, where the starting is specified by the ihfSrcAddressBegin object. Set this column to the same value as the ihfSrcAddressBegin column to get an exact single address match.

This object is only used if sourceAddress is set in ihfType."

::= { ipHeaderFilterEntry 5 }

ihfDstAddressBegin OBJECT-TYPE

SYNTAX IpsecIPAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The starting address of a destination address range that the packet must match against for this filter to be considered TRUE.

This object is only used if destinationAddress is set in ihfType."

::= { ipHeaderFilterEntry 6 }

ihfDstAddressEnd OBJECT-TYPE

SYNTAX IpsecIPAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The ending address of a destination address range to check a packet against, where the first is specified by the ihfDstAddressBegin object. Set this column to the same value as the ihfDstAddressBegin column to get an exact single address match.

This object is only used if destinationAddress is set in ihfType."

::= { ipHeaderFilterEntry 7 }

ihfSrcLowPort OBJECT-TYPE

SYNTAX Integer32 (0..65536)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The low port of the port range a packet's source must match against. To match, the port number must be greater than or equal to this value.

This object is only used if sourcePort is set in ihfType."

::= { ipHeaderFilterEntry 8 }

ihfSrcHighPort OBJECT-TYPE

SYNTAX Integer32 (0..65536)

MAX-ACCESS read-create

Various Authors

[Page 25]

Internet Draft

IPsec Policy Configuration MIB

June 2002

STATUS current

DESCRIPTION

"The high port of the port range a packet's source must match against. To match, the port number must be less than or equal to this value.

This object is only used if sourcePort is set in ihfType."

::= { ipHeaderFilterEntry 9 }

ihfDstLowPort OBJECT-TYPE

SYNTAX Integer32 (0..65536)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The low port of the port range a packet's destination must match against. To match, the port number must be greater than or equal to this value.

This object is only used if destinationPort is set in ihfType."

::= { ipHeaderFilterEntry 10 }

ihfDstHighPort OBJECT-TYPE

SYNTAX Integer32 (0..65536)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The high port of the port range a packet's destination must match against. To match, the port number must be less than or equal to this value.

This object is only used if destinationPort is set in ihfType."

```
::= { ipHeaderFilterEntry 11 }
```

ihfProtocol OBJECT-TYPE

SYNTAX Integer32 (0..255)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The protocol number the incoming packet must match against for this filter to be evaluated as true.

This object is only used if protocol is set in ihfType."

```
::= { ipHeaderFilterEntry 12 }
```

ihfIPv6FlowLabel OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(3))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The IPv6 Flow Label that the packet must match against.

This object is only used if ipv6FlowLabel is set in ihfType."

```
::= { ipHeaderFilterEntry 13 }
```

ihfLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

```
::= { ipHeaderFilterEntry 14 }
```

ihfStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

DEFVAL { nonVolatile }

```
::= { ipHeaderFilterEntry 15 }
```

```
ihfRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This object indicates the conceptual status of this row.

        This object may not be set to active if the requirements of
        the ihfType object are not met.  In other words, if the
        associated value columns needed by a particular test have not
        been set, then attempting to change this row to an active
        state will result in an inconsistentValue error.  See the
        ihfType object description for further details."
 ::= { ipHeaderFilterEntry 16 }
```

```
--
-- Time/scheduling filter table
--
```

```
timeFilterTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF TimeFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Defines a table of filters which can be used to effectively
        enable or disable policies based on a valid time range."
```

```
 ::= { ipsecPolicyConfigObjects 9 }

timeFilterEntry OBJECT-TYPE
    SYNTAX      TimeFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing a given time frame for which a policy may be
        filtered on to place the rule active or inactive."
    INDEX      { tfName }
 ::= { timeFilterTable 1 }

TimeFilterEntry ::= SEQUENCE {
    tfName          SnmpAdminString,
```

```

tfPeriodStart      DateAndTime,
tfPeriodEnd        DateAndTime,
tfMonthOfYearMask  BITS,
tfDayOfMonthMask   OCTET STRING,
tfDayOfWeekMask    BITS,
tfTimeOfDayMaskStart DateAndTime,
tfTimeOfDayMaskEnd DateAndTime,
tfLastChanged      TimeStamp,
tfStorageType       StorageType,
tfRowStatus         RowStatus
}

```

tfName OBJECT-TYPE

```

SYNTAX      SnmpAdminString (SIZE(1..32))
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "An administratively assigned name for this filter."
 ::= { timeFilterEntry 1 }

```

tfPeriodStart OBJECT-TYPE

```

SYNTAX      DateAndTime
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "The starting time period for this filter. In addition to a
    normal DateAndTime string, this object may be set to the
    OCTET STRING value THISANDPRIOR which indicates that the
    filter is valid from any time before now up until (at least)
    now."
DEFVAL { '00000101000000002b0000'H }
 ::= { timeFilterEntry 2 }

```

tfPeriodEnd OBJECT-TYPE

```

SYNTAX      DateAndTime
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "The ending time period for this filter. In addition to a
    normal DateAndTime string, this object may be set to the

```


OCTET STRING value THISANDFUTURE which indicates that the filter is valid without an ending date and/or time."
DEFVAL { '99991231235959092b0000'H }
::= { timeFilterEntry 3 }

tfMonthOfYearMask OBJECT-TYPE

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) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"A bit mask which overlays the tfPeriodStart to tfPeriodEnd date range to further restrict the time period to a restricted set of months of the year."

DEFVAL { { january, february, march, april, may, june, july, august, september, october, november, december } }

::= { timeFilterEntry 4 }

tfDayOfMonthMask OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(4))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Defines which days of the month this time period is valid for. It is a sequence of 32 BITS, where each BIT represents a corresponding day of the month starting from the left most bit being equal to the first day of the month. The last bit in the string MUST be zero."

DEFVAL { 'fffffffe'H }

::= { timeFilterEntry 5 }

tfDayOfWeekMask OBJECT-TYPE

SYNTAX BITS { monday(0), tuesday(1), wednesday(2), thursday(3),
friday(4), saturday(5), sunday(6) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"A bit mask which overlays the tfPeriodStart to tfPeriodEnd date range to further restrict the time period to a restricted

```
    set of days within a given week."
DEFVAL { { monday, tuesday, wednesday, thursday, friday,
          saturday, sunday } }
::= { timeFilterEntry 6 }
```

tfTimeOfDayMaskStart OBJECT-TYPE

SYNTAX DateAndTime

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Indicates the starting time of day for which this filter evaluates to true. The date portions of the DateAndTime TC are ignored for purposes of evaluating this mask and only the time specific portions are used."

DEFVAL { '000000000000000000002b0000'H }

::= { timeFilterEntry 7 }

tfTimeOfDayMaskEnd OBJECT-TYPE

SYNTAX DateAndTime

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Indicates the ending time of day for which this filter evaluates to true. The date portions of the DateAndTime TC are ignored for purposes of evaluating this mask and only the time specific portions are used. If this starting and ending time values indicated by the tfTimeOfDayMaskStart and tfTimeOfDayMaskEnd objects are equal, the filter is expected to be evaluated over the entire 24 hour period."

DEFVAL { '000000000000000000002b0000'H }

::= { timeFilterEntry 8 }

tfLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { timeFilterEntry 9 }

tfStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were

Internet Draft

IPsec Policy Configuration MIB

June 2002

created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

```
DEFVAL { nonVolatile }
 ::= { timeFilterEntry 10 }
```

tfRowStatus OBJECT-TYPE

```
SYNTAX      RowStatus
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
```

```
    "This object indicates the conceptual status of this row."
 ::= { timeFilterEntry 11 }
```

```
--
-- IPSO protection authority filtering
--
```

ipsoHeaderFilterTable OBJECT-TYPE

```
SYNTAX      SEQUENCE OF IpsoHeaderFilterEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
```

```
    "This table contains a list of IPSO header filter definitions
    to be used within the policyRuleDefinitionTable or the
    filtersInCompoundFilter table. IPSO headers and their values
    are described in RFC1108."
 ::= { ipsecPolicyConfigObjects 10 }
```

ipsoHeaderFilterEntry OBJECT-TYPE

```
SYNTAX      IpsoHeaderFilterEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
```

```
    "A definition of a particular filter."
INDEX      { ipsohfName }
 ::= { ipsoHeaderFilterTable 1 }
```

IpsoHeaderFilterEntry ::= SEQUENCE {

```
    ipsohfName                SnmpAdminString,
    ipsohfType                 BITS,
    ipsohfClassification      INTEGER,
```

```

    ipsohfProtectionAuth          INTEGER,
    ipsohfLastChanged            TimeStamp,
    ipsohfStorageType            StorageType,
    ipsohfRowStatus              RowStatus
}

```

```

ipsohfName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The administrative name for this filter."
    ::= { ipsoHeaderFilterEntry 1 }

ipsohfType OBJECT-TYPE
    SYNTAX      BITS { classificationLevel(0), protectionAuthority(1) }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The IPSO header fields to match the value against."
    ::= { ipsoHeaderFilterEntry 2 }

ipsohfClassification OBJECT-TYPE
    SYNTAX      INTEGER { topSecret(61), secret(90),
                        confidential(150), unclassified(171) }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The IPSO classification header field value must match the
         value in this column if the classificationLevel bit is set in
         the ipsohfType field."
    ::= { ipsoHeaderFilterEntry 3 }

ipsohfProtectionAuth OBJECT-TYPE
    SYNTAX      INTEGER { genser(0), siopesi(1), sci(2), nsa(3), doe(4) }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The IPSO protection authority header field value must match
         the value in this column if the protection authority bit is
         set in the ipsohfType field."
    ::= { ipsoHeaderFilterEntry 4 }

```

ipsohfLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or created
either through SNMP SETs or by some other external means."
::= { ipsoHeaderFilterEntry 5 }

ipsohfStorageType OBJECT-TYPE
SYNTAX StorageType

MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The storage type for this row. Rows in this table which were
created through an external process may have a storage type of
readOnly or permanent. Entries which are permanent are
expected to have at least one configurable column in the row, but
which columns are in fact modifiable is implementation specific."
DEFVAL { nonVolatile }
::= { ipsoHeaderFilterEntry 6 }

ipsohfRowStatus OBJECT-TYPE
SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object indicates the conceptual status of this row.

This object may not be set to active if the requirements of
the ipsohfType object are not met. In other words, if the
associated value columns needed by a particular test have not
been set, then attempting to change this row to an active
state will result in an inconsistentValue error. See the
ipsohfType object description for further details."
::= { ipsoHeaderFilterEntry 7 }

--
-- credential filter table
--

credentialFilterTable OBJECT-TYPE

SYNTAX SEQUENCE OF CredentialFilterEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This table defines filters which can be used to match credentials of IKE peers, where the credentials in question have been obtained from an IKE phase 1 exchange. They may be X.509 certificates, Kerberos tickets, etc..."

::= { ipsecPolicyConfigObjects 11 }

credentialFilterEntry OBJECT-TYPE

SYNTAX CredentialFilterEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A row defining a particular credential filter"

INDEX { crfName }

::= { credentialFilterTable 1 }

CredentialFilterEntry ::= SEQUENCE {

crfName SnmpAdminString,

crfCredentialType INTEGER,

crfMatchFieldName OCTET STRING,

crfMatchFieldValue OCTET STRING,

crfAcceptCredFrom OCTET STRING,

crfLastChanged TimeStamp,

crfStorageType StorageType,

crfRowStatus RowStatus

}

crfName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(1..32))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The administrative name of this filter."

::= { credentialFilterEntry 1 }

crfCredentialType OBJECT-TYPE

SYNTAX INTEGER { x509(1), kerberos(2) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The credential type that is expected for this filter to succeed."
DEFVAL { x509 }
::= { credentialFilterEntry 2 }

crfMatchFieldName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..4096))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The piece of the credential to match against. Examples:
serialNumber, signatureAlgorithm, issuerName, subjectName, ..."
::= { credentialFilterEntry 3 }

crfMatchFieldValue OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..4096))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The value that the field indicated by the crfMatchFieldName
must match against for the filter to be considered TRUE."
::= { credentialFilterEntry 4 }

crfAcceptCredFrom OBJECT-TYPE
SYNTAX OCTET STRING(SIZE(1..117))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This value is used to look up a row in the
ipsecCredMngServiceTable for the Certificate Authority
Information. This value is empty if there is no CA used for
this filter."
::= { credentialFilterEntry 5 }

crfLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { credentialFilterEntry 6 }

crfStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

DEFVAL { nonVolatile }

::= { credentialFilterEntry 7 }

crfRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row."

::= { credentialFilterEntry 8 }

--

-- Peer Identity Filter Table

--

peerIdentityFilterTable OBJECT-TYPE

SYNTAX SEQUENCE OF PeerIdentityFilterEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This table defines filters which can be used to match credentials of IKE peers, where the credentials in question have been obtained from an IKE phase 1 exchange. They may be X.509 certificates, Kerberos tickets, etc..."

::= { ipsecPolicyConfigObjects 12 }


```
peerIdentityFilterEntry OBJECT-TYPE
    SYNTAX      PeerIdentityFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row defining a particular credential filter"
    INDEX      { pifName }
    ::= { peerIdentityFilterTable 1 }
```

```
PeerIdentityFilterEntry ::= SEQUENCE {
    pifName                SnmpAdminString,
    pifIdentityType        IpsecDoiIdentType,
    pifIdentityValue       OCTET STRING,
    pifLastChanged         TimeStamp,
    pifStorageType         StorageType,
    pifRowStatus           RowStatus
}
```

```
pifName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The administrative name of this filter."
    ::= { peerIdentityFilterEntry 1 }
```

```
pifIdentityType OBJECT-TYPE
    SYNTAX      IpsecDoiIdentType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The type of identity field in the peer ID payload to match
        against."
    ::= { peerIdentityFilterEntry 2 }
```

```
pifIdentityValue OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(1..4096))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
```

"The value that the peer ID payload value must match against."

Wildcard mechanisms MUST be supported such that:

- a pifIdentityValue of '*@company.com' will match a userFqdn ID payload of 'JDOE@COMPANY.COM'
- a pifIdentityValue of '*.company.com' will match a fqdn ID payload of 'WWW.COMPANY.COM'
- a pifIdentityValue 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'
- a pifIdentityValue of '193.190.125.0/24' will match an IPv4 address ID payload of 193.190.125.10
- a pifIdentityValue of '193.190.125.*' will also match an IPv4 address ID payload of 193.190.125.10.

The character '*' replaces 0 or multiple instances of any character."

```
::= { peerIdentityFilterEntry 3 }
```

pifLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

```
::= { peerIdentityFilterEntry 4 }
```

pifStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

DEFVAL { nonVolatile }

```
::= { peerIdentityFilterEntry 5 }
```

pifRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

```
STATUS      current
DESCRIPTION
    "This object indicates the conceptual status of this row.
    This object can not be considered active unless the
    pifIdentityType and pifIdentityValue column values are
    defined."
 ::= { peerIdentityFilterEntry 6 }

--
-- compound actions table
--

compoundActionsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CompoundActionsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Table used to allow multiple actions to be associated with a
        rule. It uses the actionsInCompoundActionsTable to do this."
    ::= { ipsecPolicyConfigObjects 13 }

compoundActionsEntry OBJECT-TYPE
    SYNTAX      CompoundActionsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row in the compoundActionsTable."
    INDEX      { caName }
    ::= { compoundActionsTable 1 }

CompoundActionsEntry ::= SEQUENCE {
    caName                               SnmpAdminString,
    caExecutionStrategy                  INTEGER,
    caLastChanged                         TimeStamp,
    caStorageType                         StorageType,
    caRowStatus                           RowStatus
}

caName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This is an administratively assigned name of this compound action."
    ::= { compoundActionsEntry 1 }
```

caExecutionStrategy OBJECT-TYPE
SYNTAX INTEGER { reserved(0),

```
doAll(1),
doUntilSuccess(2),
doUntilFailure(3) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
    "This object indicates how the sub-actions are executed based
    on the success of the actions as they finish executing.

doAll - run each sub-action regardless of the exit
status of the previous action. This parent
action is always considered to have acted
successfully.

doUntilSuccess - run each sub-action until one succeeds, at
which point stop processing the sub-actions
within this parent compound action. If one
of the sub-actions did execute
successfully, this parent action is also
considered to have executed successfully.

doUntilFailure - run each sub-action until one fails, at
which point stop processing the sub-actions
within this compound action. If any
sub-action fails, the result of this parent
action is considered to have failed."
DEFVAL { doUntilSuccess }
 ::= { compoundActionsEntry 2 }
```

caLastChanged OBJECT-TYPE

```
SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
```

```
"The value of sysUpTime when this row was last modified or created
either through SNMP SETs or by some other external means."
 ::= { compoundActionsEntry 3 }
```

caStorageType OBJECT-TYPE

SYNTAX StorageType
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

Various Authors

[Page 39]

Internet Draft

IPsec Policy Configuration MIB

June 2002

DEFVAL { nonVolatile }
 ::= { compoundActionsEntry 4 }

caRowStatus OBJECT-TYPE

SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other objects in this conceptual row can be modified.

Once a row in the compoundActionsTable has been made active, this object may not be set to destroy without first destroying all the contained rows listed in the actionsInCompoundActionsTable."

::= { compoundActionsEntry 5 }

--

-- actions contained within a compound action

--

actionsInCompoundActionsTable OBJECT-TYPE

SYNTAX SEQUENCE OF ActionsInCompoundActionsEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

"This table contains a list of the sub-actions within a given compound action. Compound actions executing these actions MUST execute them in series based on the aicaPriority value,

with the lowest value executing first."
 ::= { ipsecPolicyConfigObjects 14 }

actionsInCompoundActionsEntry OBJECT-TYPE
SYNTAX ActionsInCompoundActionsEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "A row containing a reference to a given compound-action
 sub-action."
INDEX { caName, aicaPriority }
 ::= { actionsInCompoundActionsTable 1 }

ActionsInCompoundActionsEntry ::= SEQUENCE {
 aicaPriority Integer32,
 aicaSubActionName VariablePointer,

Various Authors

[Page 40]

Internet Draft

IPsec Policy Configuration MIB

June 2002

aicaLastChanged TimeStamp,
aicaStorageType StorageType,
aicaRowStatus RowStatus
}

aicaPriority OBJECT-TYPE
SYNTAX Integer32 (0..65536)
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "The priority of a given sub-action within a compound action.
 The order in which sub-actions should be executed are based on
 the value from this column, with the lowest numeric value
 executing first."
 ::= { actionsInCompoundActionsEntry 1 }

aicaSubActionName OBJECT-TYPE
SYNTAX VariablePointer
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "This column points to the action to be taken. It may, but is
 not limited to, point to a row in one of the following
 tables:

compoundActionsTable - Allowing recursion
saPreconfiguredActionTable
ikeActionTable
ipsecActionTable

It may also point to one of the scalar objects beneath saStaticActions.

If this object is set to a pointer to a row in an unsupported (or unknown) table, an inconsistentValue error should be returned.

If this object is set to point to a non-existent row in an otherwise supported table, an inconsistentName error should be returned."

::= { actionsInCompoundActionsEntry 2 }

aicaLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created

either through SNMP SETs or by some other external means."

::= { actionsInCompoundActionsEntry 3 }

aicaStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

DEFVAL { nonVolatile }

::= { actionsInCompoundActionsEntry 4 }

aicaRowStatus OBJECT-TYPE

SYNTAX RowStatus

```

MAX-ACCESS read-create
STATUS current
DESCRIPTION
    "This object indicates the conceptual status of this row.

    The value of this object has no effect on whether other
    objects in this conceptual row can be modified."
 ::= { actionsInCompoundActionsEntry 5 }

--
-- Static Actions
--

-- these are static actions which can be pointed to by the pRuleAction
-- or the aicaSubActionName objects to drop, accept or reject packets.

saStaticActions OBJECT IDENTIFIER ::= { ipsecPolicyConfigObjects 15 }

saDropAction OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "This scalar indicates that a packet should be dropped WITHOUT
        action/packet logging. This object returns a value
        of 1 for IPsec policy implementations that support the drop
        static action."
    ::= { saStaticActions 1 }

saDropActionLog OBJECT-TYPE

```

```

SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "This scalar indicates that a packet should be dropped WITH
    action/packet logging. This object returns a value
    of 1 for IPsec policy implementations that support the drop
    static action with logging."
 ::= { saStaticActions 2 }

saAcceptAction OBJECT-TYPE

```


SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"This Scalar indicates that a packet should be accepted (pass-through) WITHOUT action/packet logging. This object returns a value of 1 for IPsec policy implementations that support the accept static action."

::= { saStaticActions 3 }

saAcceptActionLog OBJECT-TYPE

SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"This scalar indicates that a packet should be accepted (pass-through) WITH action/packet logging. This object returns a value of 1 for IPsec policy implementations that support the accept static action with logging."

::= { saStaticActions 4 }

saRejectIKEAction OBJECT-TYPE

SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"This scalar indicates that a packet should be rejected WITHOUT action/packet logging. This object returns a value of 1 for IPsec policy implementations that support the reject static action."

::= { saStaticActions 5 }

saRejectIKEActionLog OBJECT-TYPE

SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"This scalar indicates that a packet should be rejected WITH action/packet logging. This object returns a value of 1 for IPsec policy implementations that support the reject static action with logging."

```

 ::= { saStaticActions 6 }

--
-- Preconfigured Action Table
--

saPreconfiguredActionTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SaPreconfiguredActionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table is a list of non-negotiated IPsec actions (SAs) that
         can be performed and contains or indicates the data necessary
         to create such an SA."
    ::= { ipsecPolicyConfigObjects 16 }

saPreconfiguredActionEntry OBJECT-TYPE
    SYNTAX      SaPreconfiguredActionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "One entry in the saPreconfiguredActionTable."
    INDEX       { sapActionName, sapSADirection }
    ::= { saPreconfiguredActionTable 1 }

SaPreconfiguredActionEntry ::= SEQUENCE {
    sapActionName                SnmpAdminString,
    sapSADirection               IpsecSADirection,
    sapActionDescription         OCTET STRING,
    sapActionLifetimeSec        Unsigned32,
    sapActionLifetimeKB         Unsigned32,
    sapDoActionLogging          TruthValue,
    sapDoPacketLogging          TruthValue,
    sapDFHandling               INTEGER,
    sapActionType               IpsecDoiEncapsulationMode,
    sapAHSPI                    Integer32,
    sapAHTransformName          SnmpAdminString,
    sapAHSharedSecretName       SnmpAdminString,
    sapESPSPPI                  Integer32,
    sapESPTransformName         SnmpAdminString,
    sapESPEncSharedSecretName   SnmpAdminString,
    sapESPAuthSharedSecretName  SnmpAdminString,

```

```

    sapIPCompSPI                      Integer32,
    sapIPCompTransformName            SnmpAdminString,
    sapPeerGatewayIdName              OCTET STRING,
    sapLastChanged                    TimeStamp,
    sapStorageType                    StorageType,
    sapRowStatus                      RowStatus
}

sapActionName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This object contains the name of this SaPreconfiguredActionEntry."
    ::= { saPreconfiguredActionEntry 1 }

sapSADirection OBJECT-TYPE
    SYNTAX      IpsecSADirection
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This object indicates whether a row should apply to outgoing
         or incoming SAs"
    ::= { saPreconfiguredActionEntry 2 }

sapActionDescription OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..255))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "An administratively assigned string which may be used
         to describe what the action does."
    DEFVAL { "" }
    ::= { saPreconfiguredActionEntry 3 }

sapActionLifetimeSec OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "sapActionLifetimeKB specifies how long in seconds the security
         association derived from this action should be used. The
         default lifetime is 8 hours. A value of 0 indicates no limit
         on the lifetime of the SA."
    DEFVAL      { 28800 }
    ::= { saPreconfiguredActionEntry 4 }
```

sapActionLifetimeKB OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"sapActionLifetimeKB specifies how long in kilobytes the security association derived from this action should be used. The default value, '0', indicates no kilobyte limit."

DEFVAL { 0 }
 ::= { saPreconfiguredActionEntry 5 }

sapDoActionLogging OBJECT-TYPE

SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"sapDoActionLogging specifies whether or not an audit message should be logged when a preconfigured SA is created."

DEFVAL { false }
 ::= { saPreconfiguredActionEntry 6 }

sapDoPacketLogging OBJECT-TYPE

SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"sapDoPacketLogging specifies whether or not an audit message should be logged when a packet is passed through the SA."

DEFVAL { false }
 ::= { saPreconfiguredActionEntry 7 }

sapDFHandling OBJECT-TYPE

SYNTAX INTEGER {
 reserved(0), -- reserved
 copy(1), -- indicates copy the DF bit from the
 -- internal to external IP header.
 set(2), -- set the DF bit in the external IP
 -- header to 1.
 clear(3) -- clear the DF bit in the external IP
 -- header to 0.

```
    }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
    "This object specifies how to process the DF bit in packets
    sent through the preconfigured SA. This object is not used
    for transport SAs."
DEFVAL { copy }
```

```
::= { saPreconfiguredActionEntry 8 }
```

sapActionType OBJECT-TYPE

SYNTAX IsecDoiEncapsulationMode

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies the encapsulation mode to use for the
preconfigured SA: tunnel or transport mode."

DEFVAL { tunnel }

```
::= { saPreconfiguredActionEntry 9 }
```

sapAHSPI OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object represents the SPI value for the AH SA."

```
::= { saPreconfiguredActionEntry 10 }
```

sapAHTransformName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object is the name of the AH transform to use as an
index into the AHTransformTable. A zero length value
indicates no transform of this type is used."

```
::= { saPreconfiguredActionEntry 11 }
```

sapAHSharedSecretName OBJECT-TYPE

SYNTAX SnmpAdminString(SIZE(0..32))

MAX-ACCESS read-create

STATUS current
DESCRIPTION
"This object contains a name value to be used as an index into
the keyTable which holds the pertinent keying
information for the AH SA."
 ::= { saPreconfiguredActionEntry 12 }

sapESPSPi OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object represents the SPI value for the ESP SA."
 ::= { saPreconfiguredActionEntry 13 }

Various Authors

[Page 47]

Internet Draft

IPsec Policy Configuration MIB

June 2002

sapESPTransformName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(0..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object is the name of the ESP transform to use as an
index into the ESPTransformTable. A zero length value
indicates no transform of this type is used."
 ::= { saPreconfiguredActionEntry 14 }

sapESPEncSharedSecretName OBJECT-TYPE
SYNTAX SnmpAdminString(SIZE(0..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object contains a name value to be used as an index into
the keyTable which holds the pertinent keying
information for the encryption algorithm of the ESP SA."
 ::= { saPreconfiguredActionEntry 15 }

sapESPAuthSharedSecretName OBJECT-TYPE
SYNTAX SnmpAdminString(SIZE(0..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object contains a name value to be used as an index into

the keyTable which holds the pertinent keying information for the authentication algorithm of the ESP SA."
 ::= { saPreconfiguredActionEntry 16 }

sapIPCompSPI OBJECT-TYPE

SYNTAX Integer32
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object represents the SPI value for the IPComp SA."

::= { saPreconfiguredActionEntry 17 }

sapIPCompTransformName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(0..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object is the name of the IPComp transform to use as an index into the IPCompTransformTable. A zero length value indicates no transform of this type is used."

::= { saPreconfiguredActionEntry 18 }

sapPeerGatewayIdName OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..116))
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the peer id name of the peer gateway. This object can be used to look up the peer id value, address and other values in the peerIdentityTable. This object is used when initiating a tunnel SA. This object is not used for transport SAs. If sapActionType specifies tunnel mode and this object is empty, the peer gateway should be determined from the source or destination of the packet."

DEFVAL { "" }

::= { saPreconfiguredActionEntry 19 }

sapLastChanged OBJECT-TYPE

SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { saPreconfiguredActionEntry 20 }

sapStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

DEFVAL { nonVolatile }

::= { saPreconfiguredActionEntry 21 }

sapRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other objects in this conceptual row can be modified.

If active, this object must remain active if it is referenced

by a row in another table."

::= { saPreconfiguredActionEntry 22 }

--

-- saNegotiationParametersTable

--

-- PROPERTIES MinLifetimeSeconds

-- MinLifetimeKilobytes

-- RefreshThresholdSeconds

-- RefreshThresholdKilobytes


```

--                               IdleDurationSeconds

saNegotiationParametersTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF SaNegotiationParametersEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "This table contains reusable parameters that can be pointed
        to by the ikeActionTable and ipsecActionTable. These
        parameters are reusable since it is likely an administrator
        will want to make global policy changes to lifetime
        parameters that apply to multiple actions. This table allows
        multiple rows in the other actions tables to reuse global
        lifetime parameters in this table by repeatedly pointing to a
        row contained within this table."
    ::= { ipsecPolicyConfigObjects 17 }

saNegotiationParametersEntry OBJECT-TYPE
    SYNTAX          SaNegotiationParametersEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Contains the attributes of one row in the
        saNegotiationParametersTable."
    INDEX           { sanActionParametersName }
    ::= { saNegotiationParametersTable 1 }

SaNegotiationParametersEntry ::= SEQUENCE {
    sanActionParametersName          SnmpAdminString,
    sanMinimumLifetimeSeconds        Integer32,
    sanMinimumLifetimeKB             Integer32,
    sanRefreshThresholdSeconds       Integer32,
    sanRefreshThresholdKB            Integer32,
    sanIdleDurationSeconds           Integer32,
    sanLastChanged                   TimeStamp,
    sanStorageType                   StorageType,
}

```

```

    sanRowStatus                      RowStatus
}

```

```

sanActionParametersName OBJECT-TYPE
    SYNTAX          SnmpAdminString (SIZE(1..32))

```

MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "This object contains the administrative name of this
 SaNegotiationParametersEntry. This row can be referred
 to by this name in other policy action tables."
 ::= { saNegotiationParametersEntry 1 }

sanMinimumLifetimeSeconds OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "sanMinimumLifetimeSeconds specifies the minimum seconds
 lifetime that will be accepted from the peer."
 ::= { saNegotiationParametersEntry 2 }

sanMinimumLifetimeKB OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "sanMinimumLifetimeKB specifies the minimum kilobyte
 lifetime that will be accepted from the peer."
 ::= { saNegotiationParametersEntry 3 }

sanRefreshThresholdSeconds OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "sanRefreshThresholdSeconds specifies what percentage of
 the seconds lifetime can expire before IKE should attempt to
 renegotiate the IPsec security association.
 A value between 1 and 100 representing a percentage. A
 value of 100 indicates that the IPsec security
 association should not be renegotiated until the
 seconds lifetime has been reached."
 ::= { saNegotiationParametersEntry 4 }

sanRefreshThresholdKB OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-create

STATUS current

DESCRIPTION

"sanRefreshThresholdKB specifies what percentage of the kilobyte lifetime can expire before IKE should attempt to renegotiate the IPsec security association. A value between 1 and 100 representing a percentage. A value of 100 indicates that the IPsec security association should not be renegotiated until the kilobyte lifetime has been reached."

::= { saNegotiationParametersEntry 5 }

sanIdleDurationSeconds OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"sanIdleDurationSeconds specifies how many seconds a security association may remain idle (i.e., no traffic protected using the security association) before it is deleted. A value of zero indicates that idle detection should not be used for the security association. Any non-zero value indicates the number of seconds the security association may remain unused."

::= { saNegotiationParametersEntry 6 }

sanLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { saNegotiationParametersEntry 7 }

sanStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

DEFVAL { nonVolatile }

::= { saNegotiationParametersEntry 8 }

sanRowStatus OBJECT-TYPE

Internet Draft

IPsec Policy Configuration MIB

June 2002

```
SYNTAX      RowStatus
MAX-ACCESS  read-create
STATUS      current
```

DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other objects in this conceptual row can be modified.

This object may not be set to destroy if referred to by other rows in other action tables."

```
::= { saNegotiationParametersEntry 9 }
```

```
--
```

```
-- ikeActionTable
```

```
--
```

ikeActionTable OBJECT-TYPE

```
SYNTAX      SEQUENCE OF IkeActionEntry
MAX-ACCESS  not-accessible
STATUS      current
```

DESCRIPTION

"The ikeActionTable contains a list of the parameters used for an IKE phase 1 SA DOI negotiation. See the corresponding table ikeActionProposalsTable for a list of proposals contained within a given IKE Action."

```
::= { ipsecPolicyConfigObjects 18 }
```

ikeActionEntry OBJECT-TYPE

```
SYNTAX      IkeActionEntry
MAX-ACCESS  not-accessible
STATUS      current
```

DESCRIPTION

"The ikeActionEntry lists the IKE negotiation attributes."

```
INDEX      { ikeActionName }
```

```
::= { ikeActionTable 1 }
```

IkeActionEntry ::= SEQUENCE {

```
ikeActionName          SnmpAdminString,
ikeActionParametersName SnmpAdminString,
ikeThresholdDerivedKeys Integer32,
ikeExchangeMode        INTEGER,
```

ikeAgressiveModeGroupId	IkeGroupDescription,
ikeIdentityType	IpsecDoiIdentType,
ikeIdentityContext	SnmpAdminString,
ikePeerName	SnmpAdminString,
ikeActionDoActionLogging	TruthValue,
ikeActionDoPacketLogging	TruthValue,

ikeActionVendorId	OCTET STRING,
ikeActionLastChanged	TimeStamp,
ikeActionStorageType	StorageType,
ikeActionRowStatus	RowStatus

}

ikeActionName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(1..32))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This object contains the name of this ikeAction entry."

::= { ikeActionEntry 1 }

ikeActionParametersName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(1..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object is administratively assigned to reference a row in the saNegotiationParametersTable where additional parameters affecting this action may be found."

::= { ikeActionEntry 2 }

ikeThresholdDerivedKeys OBJECT-TYPE

SYNTAX Integer32 (0..100)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ikeThresholdDerivedKeys specifies what percentage of the derived key limit (see the LifetimeDerivedKeys property of IKEProposal) can expire before IKE should attempt to renegotiate the IKE phase 1 security association."

DEFVAL { 100 }

::= { ikeActionEntry 3 }

ikeExchangeMode OBJECT-TYPE
SYNTAX INTEGER { main(1), aggressive(2) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ikeExchangeMode specifies the IKE Phase 1 negotiation mode."
DEFVAL { main }
::= { ikeActionEntry 4 }

ikeAggressiveModeGroupId OBJECT-TYPE
SYNTAX IkeGroupDescription
MAX-ACCESS read-create

STATUS current
DESCRIPTION
"The values to be used for Diffie-Hellman exchange."
::= { ikeActionEntry 5 }

ikeIdentityType OBJECT-TYPE
SYNTAX IsecDoiIdentType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This column along with ikeIdentityContext and endpoint
information is used to refer an ikeIdentityEntry in the
ikeIdentityTable."
::= { ikeActionEntry 6 }

ikeIdentityContext OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This column, along with ikeIdentityType and endpoint
information, is used to refer to an ikeIdentityEntry in the
ikeIdentityTable."
::= { ikeActionEntry 7 }

ikePeerName OBJECT-TYPE
SYNTAX SnmpAdminString(SIZE(1..116))
MAX-ACCESS read-create

STATUS current
DESCRIPTION
"This object indicates the peer id name of the IKE peer. This object can be used to look up the peer id value, address, keys and other values in the peerIdentityTable."
 ::= { ikeActionEntry 8 }

ikeActionDoActionLogging OBJECT-TYPE

SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ikeDoActionLogging specifies whether or not an audit message should be logged when this ike SA is created."
DEFVAL { false }
 ::= { ikeActionEntry 9 }

ikeActionDoPacketLogging OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ikeDoPacketLogging specifies whether or not an audit message should be logged when a packet is passed through the SA."
DEFVAL { false }
 ::= { ikeActionEntry 10 }

ikeActionVendorId OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..65535))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"Vendor ID Payload. A value of NULL means that Vendor ID payload will be neither generated nor accepted. A non-NULL value means that a Vendor ID payload will be generated (when acting as an initiator) or is expected (when acting as a responder)."
DEFVAL { "" }
 ::= { ikeActionEntry 11 }

ikeActionLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or created
either through SNMP SETs or by some other external means."
 ::= { ikeActionEntry 12 }

ikeActionStorageType OBJECT-TYPE
SYNTAX StorageType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The storage type for this row. Rows in this table which were
created through an external process may have a storage type of
readOnly or permanent. Entries which are permanent are
expected to have at least one configurable column in the row, but
which columns are in fact modifiable is implementation specific."
DEFVAL { nonVolatile }
 ::= { ikeActionEntry 13 }

ikeActionRowStatus OBJECT-TYPE
SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other
objects in this conceptual row can be modified.

This object may not be set to destroy if referred to by other
rows in other action tables."

::= { ikeActionEntry 14 }

--

-- ikeActionProposalsTable proposals contained within a ikeAction

--

ikeActionProposalsTable OBJECT-TYPE

SYNTAX SEQUENCE OF IkeActionProposalsEntry
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 "This table contains a list of all ike proposal names found
 within a given IKE Action."
 ::= { ipsecPolicyConfigObjects 19 }

ikeActionProposalsEntry OBJECT-TYPE
 SYNTAX IkeActionProposalsEntry
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 "a row containing one ike proposal reference"
 INDEX { ikeActionName, ikeActionProposalPriority }
 ::= { ikeActionProposalsTable 1 }

IkeActionProposalsEntry ::= SEQUENCE {
 ikeActionProposalPriority Integer32,
 ikeActionProposalName SnmpAdminString,
 ikeActionProposalLastChanged TimeStamp,
 ikeActionProposalStorageType StorageType,
 ikeActionProposalRowStatus RowStatus
 }

ikeActionProposalPriority OBJECT-TYPE
 SYNTAX Integer32 (0..65535)
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 "The numeric priority of a given contained proposal inside an
 ike Action. This index should be used to order the proposals
 in an IKE Phase I negotiation, lowest value first."
 ::= { ikeActionProposalsEntry 1 }

ikeActionProposalName OBJECT-TYPE
 SYNTAX SnmpAdminString (SIZE(1..32))
 MAX-ACCESS read-create
 STATUS current
 DESCRIPTION
 "The administratively assigned name that can be used to
 reference a set of values contained within the

```

        ikeProposalTable."
 ::= { ikeActionProposalsEntry 2 }

ikeActionProposalLastChanged OBJECT-TYPE
    SYNTAX          TimeStamp
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The value of sysUpTime when this row was last modified or created
        either through SNMP SETs or by some other external means."
 ::= { ikeActionProposalsEntry 3 }

ikeActionProposalStorageType OBJECT-TYPE
    SYNTAX          StorageType
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The storage type for this row.  Rows in this table which were
        created through an external process may have a storage type of
        readOnly or permanent.  Entries which are permanent are
        expected to have at least one configurable column in the row, but
        which columns are in fact modifiable is implementation specific."
    DEFVAL { nonVolatile }
 ::= { ikeActionProposalsEntry 4 }

ikeActionProposalRowStatus OBJECT-TYPE
    SYNTAX          RowStatus
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This object indicates the conceptual status of this row.

        The value of this object has no effect on whether other
        objects in this conceptual row can be modified."
 ::= { ikeActionProposalsEntry 5 }

--
-- IKE proposal definition table
--

```

```

ikeProposalTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IkeProposalEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table contains a list of IKE proposals which are used in an
        IKE negotiation."
    ::= { ipsecPolicyConfigObjects 20 }

```

```

ikeProposalEntry OBJECT-TYPE
    SYNTAX      IkeProposalEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "One IKE proposal entry."
    INDEX       { ikeActionProposalName }
    ::= { ikeProposalTable 1 }

```

```

IkeProposalEntry ::= SEQUENCE {
    ipLifetimeDerivedKeys          Unsigned32,
    ipCipherAlgorithm              IkeEncryptionAlgorithm,
    ipCipherKeyLength              Unsigned32,
    ipCipherKeyRounds              Unsigned32,
    ipHashAlgorithm                IkeHashAlgorithm,
    ipPrfAlgorithm                 INTEGER,
    ipVendorId                     OCTET STRING,
    ipDhGroup                       IkeGroupDescription,
    ipAuthenticationMethod         IkeAuthMethod,
    ipMaxLifetimeSeconds           Unsigned32,
    ipMaxLifetimeKB                Unsigned32,
    ipProposalLastChanged          TimeStamp,
    ipProposalStorageType          StorageType,
    ipProposalRowStatus            RowStatus
}

```

```

ipLifetimeDerivedKeys OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "ipLifetimeDerivedKeys specifies the number of times that
        a phase 1 key will be used to derive a phase 2 key before the
        phase 1 security association needs renegotiated."
    ::= { ikeProposalEntry 1 }

```

```

ipCipherAlgorithm OBJECT-TYPE
    SYNTAX      IkeEncryptionAlgorithm
    MAX-ACCESS  read-create

```

Internet Draft

IPsec Policy Configuration MIB

June 2002

STATUS current

DESCRIPTION

"ipCipherAlgorithm specifies the proposed phase 1 security association encryption algorithm."

::= { ikeProposalEntry 2 }

ipCipherKeyLength OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies, in bits, the key length for the cipher algorithm used in IKE Phase 1 negotiation."

::= { ikeProposalEntry 3 }

ipCipherKeyRounds OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies the number of key rounds for the cipher algorithm used in IKE Phase 1 negotiation."

::= { ikeProposalEntry 4 }

ipHashAlgorithm OBJECT-TYPE

SYNTAX IkeHashAlgorithm

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipHashAlgorithm specifies the proposed phase 1 security association hash algorithm."

::= { ikeProposalEntry 5 }

ipPrfAlgorithm OBJECT-TYPE

SYNTAX INTEGER { reserved(0) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipPRFAlgorithm specifies the proposed phase 1 security association psuedo-random function.

Note: currently no prf algorithms are defined."

::= { ikeProposalEntry 6 }

ipVendorId OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-create
STATUS current

Various Authors

[Page 60]

Internet Draft

IPsec Policy Configuration MIB

June 2002

DESCRIPTION

"The VendorID property is used to identify vendor-defined key exchange GroupIDs."

::= { ikeProposalEntry 7 }

ipDhGroup OBJECT-TYPE

SYNTAX IkeGroupDescription
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"This object specifies the proposed phase 1 security association Diffie-Hellman group"

::= { ikeProposalEntry 8 }

ipAuthenticationMethod OBJECT-TYPE

SYNTAX IkeAuthMethod
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"This object specifies the proposed authentication method for the phase 1 security association."

::= { ikeProposalEntry 9 }

ipMaxLifetimeSeconds OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"ipMaxLifetimeSeconds specifies the maximum amount of time to propose a security association remain valid."

::= { ikeProposalEntry 10 }

ipMaxLifetimeKB OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"ipMaxLifetimeKB specifies the maximum kilobyte lifetime to propose a security association remain valid."
 ::= { ikeProposalEntry 11 }

ipProposalLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified either through SNMP SETs or by some other external means."

::= { ikeProposalEntry 12 }

ipProposalStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

::= { ikeProposalEntry 13 }

ipProposalRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other objects in this conceptual row can be modified."

::= { ikeProposalEntry 14 }

--

-- IPsec action definition table

--

```

ipsecActionTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IpsecActionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The ipsecActionTable contains a list of the parameters used for an
        IKE phase 2 IPsec DOI negotiation."
    ::= { ipsecPolicyConfigObjects 21 }

```

```

ipsecActionEntry OBJECT-TYPE
    SYNTAX      IpsecActionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The ipsecActionEntry lists the IPsec negotiation attributes."
    INDEX       { ipsecActionName }
    ::= { ipsecActionTable 1 }

```

```

IpsecActionEntry ::= SEQUENCE {
    ipsecActionName          SnmpAdminString,
    ipsecActionParametersName SnmpAdminString,
    ipsecActionProposalsName SnmpAdminString,
    ipsecUsePfs              TruthValue,
    ipsecVendorId            OCTET STRING,
    ipsecGroupId             IkeGroupDescription,
    ipsecPeerGatewayIdName  OCTET STRING,
    ipsecUseIkeGroup         TruthValue,
    ipsecGranularity         INTEGER,
    ipsecMode                INTEGER,
    ipsecDFHandling          INTEGER,
    ipsecDoActionLogging     TruthValue,
    ipsecDoPacketLogging     TruthValue,
    ipsecActionLastChanged  TimeStamp,
    ipsecActionStorageType  StorageType,
    ipsecActionRowStatus    RowStatus
}

```

```

ipsecActionName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  not-accessible

```

STATUS current
DESCRIPTION
"ipsecActionName is the name of the ipsecAction entry."
 ::= { ipsecActionEntry 1 }

ipsecActionParametersName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object is used to reference a row in the
saNegotiationActionParametersTable where additional parameters
affecting this action may be found."
 ::= { ipsecActionEntry 2 }

ipsecActionProposalsName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object is used to reference one or more rows in the
ipsecProposalsTable where an ordered list of proposals
affecting this action may be found."
 ::= { ipsecActionEntry 3 }

ipsecUsePfs OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This MIB object specifies whether or not perfect forward
secrecy should be used when refreshing keys.
A value of true indicates that PFS should be used."
 ::= { ipsecActionEntry 4 }

ipsecVendorId OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"The VendorID property is used to identify vendor-defined key exchange GroupIDs."
 ::= { ipsecActionEntry 5 }

ipsecGroupId OBJECT-TYPE

SYNTAX IkeGroupDescription

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies the Diffie-Hellman group to use for phase 2 when the object ipsecUsePfs is true and the object ipsecUseIkeGroup is false. If the GroupID number is from the vendor-specific range (32768-65535), the VendorID qualifies the group number."

::= { ipsecActionEntry 6 }

ipsecPeerGatewayIdName OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..116))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the peer id name of the peer gateway. This object can be used to look up the peer id value, address and other values in the peerIdentityTable. This object is used when initiating a tunnel SA. This object is not used for transport SAs. If no value is set and ipsecMode is tunnel, the peer gateway should be determined from the source or destination address of the packet."

::= { ipsecActionEntry 7 }

ipsecUseIkeGroup OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies whether or not to use the same GroupId for phase 2 as was used in phase 1. If UsePFS is false, this entry should be ignored."

::= { ipsecActionEntry 8 }

ipsecGranularity OBJECT-TYPE

SYNTAX INTEGER { subnet(1), address(2), protocol(3), port(4) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object specifies how the proposed selector for the security association will be created. The selector is created by using the FilterList information. The selector can be subnet, address, porotocol, or port."
 ::= { ipsecActionEntry 9 }

ipsecMode OBJECT-TYPE
SYNTAX INTEGER { tunnel(1), transport(2) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object specifies the encapsulation of the IPsec SA to be negotiated."
DEFVAL { tunnel }
 ::= { ipsecActionEntry 10 }

ipsecDFHandling OBJECT-TYPE
SYNTAX INTEGER { copy(1), set(2), clear(3) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object specifies the processing of DF bit by the negotiated IPsec tunnel.
1 - DF bit is copied.
2 - DF bit is set.
3 - DF bit is cleared."
 ::= { ipsecActionEntry 11 }

ipsecDoActionLogging OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ipsecDoActionLogging specifies whether or not an audit message should be logged when this ipsec SA is created."
DEFVAL { false }

::= { ipsecActionEntry 12 }

```

ipsecDoPacketLogging OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "ipsecDoPacketLogging specifies whether or not an audit message
        should be logged when a packet is passed through the SA."
    DEFVAL { false }
    ::= { ipsecActionEntry 13 }

ipsecActionLastChanged OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The value of sysUpTime when this row was last modified or created
        either through SNMP SETs or by some other external means."
    ::= { ipsecActionEntry 14 }

ipsecActionStorageType OBJECT-TYPE
    SYNTAX      StorageType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The storage type for this row. Rows in this table which were
        created through an external process may have a storage type of
        readOnly or permanent. Entries which are permanent are
        expected to have at least one configurable column in the row, but
        which columns are in fact modifiable is implementation specific."
    ::= { ipsecActionEntry 15 }

ipsecActionRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This object indicates the conceptual status of this row.

        The value of this object has no effect on whether other
        objects in this conceptual row can be modified.

        If active, this object must remain active if it is referenced
        by a row in another table."
    ::= { ipsecActionEntry 16 }

```

--

```
-- ipsecProposalsTable
```

```
--
```

```
ipsecProposalsTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF IpsecProposalsEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"This table lists one or more IPsec proposals for  
IPsec actions."
```

```
::= { ipsecPolicyConfigObjects 22 }
```

```
ipsecProposalsEntry OBJECT-TYPE
```

```
SYNTAX IpsecProposalsEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"An entry containing (possibly a portion of) a proposal."
```

```
INDEX { ipsecProposalsName, ipsecProposalsPriority,  
ipsecProposalsProtocolId }
```

```
::= { ipsecProposalsTable 1 }
```

```
IpsecProposalsEntry ::= SEQUENCE {
```

```
ipsecProposalsName SnmpAdminString,
```

```
ipsecProposalsPriority Integer32,
```

```
ipsecProposalsProtocolId IpsecDoiSecProtocolId,
```

```
ipsecProposalsTransformsName SnmpAdminString,
```

```
ipsecProposalsLastChanged TimeStamp,
```

```
ipsecProposalsStorageType StorageType,
```

```
ipsecProposalsRowStatus RowStatus
```

```
}
```

```
ipsecProposalsName OBJECT-TYPE
```

```
SYNTAX SnmpAdminString (SIZE(1..32))
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"The name of this proposal."
```

```
::= { ipsecProposalsEntry 1 }
```

```
ipsecProposalsPriority OBJECT-TYPE
```

```
SYNTAX Integer32 (0..65535)
```

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

```
STATUS current
```

```
DESCRIPTION
```

"The priority level (AKA sequence level) of this proposal.
A lower number indicates a higher precedence."

::= { ipsecProposalsEntry 2 }

ipsecProposalsProtocolId OBJECT-TYPE

SYNTAX IpsecDoiSecProtocolId

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The protocol Id for the transforms for this proposal. The
protoIsakmp(1) value is not valid for this object.

This object, along with the ipsecProposalsTransformsName,
is the index into the ipsecTransformsTable."

::= { ipsecProposalsEntry 3 }

ipsecProposalsTransformsName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The name of the transform or group of transforms for this
protocol. This object, along with the ipsecProposalsProtocolId,
is the index into the ipsecTransformsTable."

::= { ipsecProposalsEntry 4 }

ipsecProposalsLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created
either through SNMP SETs or by some other external means."

::= { ipsecProposalsEntry 5 }

ipsecProposalsStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were
created through an external process may have a storage type of

readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."
 ::= { ipsecProposalsEntry 6 }

ipsecProposalsRowStatus OBJECT-TYPE

SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current

Various Authors

[Page 68]

Internet Draft

IPsec Policy Configuration MIB

June 2002

DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other objects in this conceptual row can be modified.

This row may not be set to active until the corresponding row in the ipsecTransformsTable exists and is active."

::= { ipsecProposalsEntry 7 }

--

-- ipsecTransformsTable

--

ipsecTransformsTable OBJECT-TYPE

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

DESCRIPTION

"This table lists the IPsec proposals contained within a given IPsec action and the transforms within each of those proposals. These proposals and transforms can then be used to create phase 2 negotiation proposals."

::= { ipsecPolicyConfigObjects 23 }

ipsecTransformsEntry OBJECT-TYPE

SYNTAX IpsecTransformsEntry
MAX-ACCESS not-accessible
STATUS current

DESCRIPTION

"An entry containing the information on an IPsec transform."

```
INDEX      { ipsecTransformsType, ipsecTransformsName,
            ipsecTransformsPriority }
 ::= { ipsecTransformsTable 1 }
```

```
IpsecTransformsEntry ::= SEQUENCE {
    ipsecTransformsType          IpsecDoiSecProtocolId,
    ipsecTransformsName         SnmpAdminString,
    ipsecTransformsPriority      Integer32,
    ipsecTransformsTransformName SnmpAdminString,
    ipsecTransformsLastChanged  TimeStamp,
    ipsecTransformsStorageType  StorageType,
    ipsecTransformsRowStatus    RowStatus
}
```

```
ipsecTransformsType OBJECT-TYPE
    SYNTAX      IpsecDoiSecProtocolId
```

Various Authors

[Page 69]

Internet Draft

IPsec Policy Configuration MIB

June 2002

```
MAX-ACCESS not-accessible
STATUS      current
DESCRIPTION
```

```
    "The protocol type for this transform. The protoIsakmp(1) value
    is not valid for this object."
```

```
 ::= { ipsecTransformsEntry 1 }
```

```
ipsecTransformsName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS not-accessible
    STATUS      current
    DESCRIPTION
```

```
    "The name for this transform or group of transforms."
```

```
 ::= { ipsecTransformsEntry 2 }
```

```
ipsecTransformsPriority OBJECT-TYPE
    SYNTAX      Integer32 (0..65535)
    MAX-ACCESS not-accessible
    STATUS      current
    DESCRIPTION
```

```
    "The priority level (AKA sequence level) of the this transform
    within the group of transforms. This indicates the preference
    for which algorithms are requested when the list of transforms
    are sent to the remote host. A lower number indicates a higher
    precedence."
```

```
::= { ipsecTransformsEntry 3 }
```

```
ipsecTransformsTransformName OBJECT-TYPE
```

```
SYNTAX      SnmpAdminString
```

```
MAX-ACCESS  read-create
```

```
STATUS      current
```

```
DESCRIPTION
```

```
    "The name for the given transform. Depending on the value of  
    ipsecTransformsType, this value should be used to lookup  
    the transform's specific parameters in the ahTransformTable,  
    the espTransformTable or the ipcompTransformTable."
```

```
::= { ipsecTransformsEntry 4 }
```

```
ipsecTransformsLastChanged OBJECT-TYPE
```

```
SYNTAX      TimeStamp
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "The value of sysUpTime when this row was last modified or created  
    either through SNMP SETs or by some other external means."
```

```
::= { ipsecTransformsEntry 5 }
```

```
ipsecTransformsStorageType OBJECT-TYPE
```

Various Authors

[Page 70]

Internet Draft

IPsec Policy Configuration MIB

June 2002

```
SYNTAX      StorageType
```

```
MAX-ACCESS  read-create
```

```
STATUS      current
```

```
DESCRIPTION
```

```
    "The storage type for this row. Rows in this table which were  
    created through an external process may have a storage type of  
    readOnly or permanent. Entries which are permanent are  
    expected to have at least one configurable column in the row, but  
    which columns are in fact modifiable is implementation specific."
```

```
::= { ipsecTransformsEntry 6 }
```

```
ipsecTransformsRowStatus OBJECT-TYPE
```

```
SYNTAX      RowStatus
```

```
MAX-ACCESS  read-create
```

```
STATUS      current
```

```
DESCRIPTION
```

```
    "This object indicates the conceptual status of this row."
```


The value of this object has no effect on whether other objects in this conceptual row can be modified.

This row may not be set to active until the corresponding row in the ahTransformTable, espTransformTable or the ipcompTransformTable exists."

```
::= { ipsecTransformsEntry 7 }
```

```
--
```

```
-- AH transform definition table
```

```
--
```

```
ahTransformTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF AhTransformEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"This table lists all the AH transforms which can be used to build IPsec proposals."
```

```
::= { ipsecPolicyConfigObjects 24 }
```

```
ahTransformEntry OBJECT-TYPE
```

```
SYNTAX AhTransformEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"This entry contains the attributes of one AH transform."
```

```
INDEX { ahtName }
```

```
::= { ahTransformTable 1 }
```

```
AhTransformEntry ::= SEQUENCE {
```

```
  ahtName SnmpAdminString,
```

```
  ahtMaxLifetimeSec Unsigned32,
```

```
  ahtMaxLifetimeKB Unsigned32,
```

```
  ahtAlgorithm IpsecDoiAuthAlgorithm,
```

```
  ahtReplayProtection TruthValue,
```

```
  ahtReplayWindowSize Unsigned32,
```

```
  ahtLastChanged TimeStamp,
```

```
  ahtStorageType StorageType,
```

```

    ahtRowStatus          RowStatus
}

ahtName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This object contains the name of this AH transform. This row
        will be referred to by an ipsecTransformsEntry."
    ::= { ahTransformEntry 1 }

ahtMaxLifetimeSec OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "ahtMaxLifetimeSec specifies how long in seconds the security
        association derived from this transform should be used."
    ::= { ahTransformEntry 2 }

ahtMaxLifetimeKB OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "ahtMaxLifetimeKB specifies how long in kilobytes the security
        association derived from this transform should be used."
    ::= { ahTransformEntry 3 }

ahtAlgorithm OBJECT-TYPE
    SYNTAX      IpsecDoiAuthAlgorithm
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This object specifies the AH algorithm for this transform."
    ::= { ahTransformEntry 4 }

```

```

ahtReplayProtection OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-create
    STATUS      current

```

DESCRIPTION

"ahtReplayProtection indicates whether or not anti replay service is to be provided by this SA."

::= { ahTransformEntry 5 }

ahtReplayWindowSize OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ahtReplayWindowSize indicates the size, in bits, of the replay window to use if replay protection is true for this transform. The window size is assumed to be a power of two. If Replay Protection is false, this value can be ignored."

::= { ahTransformEntry 6 }

ahtLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { ahTransformEntry 7 }

ahtStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

::= { ahTransformEntry 8 }

ahtRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row."

The value of this object has no effect on whether other objects in this conceptual row can be modified.

If active, this object must remain active if it is referenced by a row in another table."

```
::= { ahTransformEntry 9 }
```

```
--
```

```
-- ESP transform definition table
```

```
--
```

```
espTransformTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF EspTransformEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"This table lists all the ESP transforms which can be used to build
IPsec proposals"
```

```
::= { ipsecPolicyConfigObjects 25 }
```

```
espTransformEntry OBJECT-TYPE
```

```
SYNTAX EspTransformEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"This entry contains the attributes of one ESP transform."
```

```
INDEX { esptName }
```

```
::= { espTransformTable 1 }
```

```
EspTransformEntry ::= SEQUENCE {
```

```
  esptName SnmpAdminString,
  esptMaxLifetimeSec Unsigned32,
  esptMaxLifetimeKB Unsigned32,
  esptCipherTransformId IpsecDoiEspTransform,
  esptCipherKeyLength Unsigned32,
  esptCipherKeyRounds Unsigned32,
  esptIntegrityAlgorithmId IpsecDoiAuthAlgorithm,
  esptReplayPrevention TruthValue,
  esptReplayWindowSize Unsigned32,
  esptLastChanged TimeStamp,
  esptStorageType StorageType,
  esptRowStatus RowStatus
```

```
}
```

```
esptName OBJECT-TYPE
```

SYNTAX SnmpAdminString (SIZE(1..32))

Various Authors

[Page 74]

Internet Draft

IPsec Policy Configuration MIB

June 2002

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The name of this particular espTransform be referred to by an ipsecTransformsEntry."

::= { espTransformEntry 1 }

esptMaxLifetimeSec OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"esptMaxLifetimeSec specifies how long in seconds the security association derived from this transform should be used."

::= { espTransformEntry 2 }

esptMaxLifetimeKB OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"esptMaxLifetimeKB specifies how long in kilobytes the security association derived from this transform should be used."

::= { espTransformEntry 3 }

esptCipherTransformId OBJECT-TYPE

SYNTAX Ipv4Addr

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies the transform ID of the ESP cipher algorithm."

::= { espTransformEntry 4 }

esptCipherKeyLength OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies, in bits, the key length for the ESP cipher algorithm."
 ::= { espTransformEntry 5 }

esptCipherKeyRounds OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current

Various Authors

[Page 75]

Internet Draft

IPsec Policy Configuration MIB

June 2002

DESCRIPTION

"This object specifies the number of key rounds for the ESP cipher algorithm."
 ::= { espTransformEntry 6 }

esptIntegrityAlgorithmId OBJECT-TYPE

SYNTAX IpsecDoiAuthAlgorithm
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"This object specifies the ESP integrity algorithm ID."
 ::= { espTransformEntry 7 }

esptReplayPrevention OBJECT-TYPE

SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"esptReplayPrevention indicates whether or not anti-replay service is to be provided by this SA."
 ::= { espTransformEntry 8 }

esptReplayWindowSize OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"esptReplayWindowSize indicates the size, in bits, of the replay window to use if replay protection is true for this transform. The window size is assumed to be a power of two. If Replay Protection is false, this value can be ignored."
 ::= { espTransformEntry 9 }

esptLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or created
either through SNMP SETs or by some other external means."
 ::= { espTransformEntry 10 }

esptStorageType OBJECT-TYPE
SYNTAX StorageType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The storage type for this row. Rows in this table which were

Various Authors

[Page 76]

Internet Draft

IPsec Policy Configuration MIB

June 2002

created through an external process may have a storage type of
readOnly or permanent. Entries which are permanent are
expected to have at least one configurable column in the row, but
which columns are in fact modifiable is implementation specific."
 ::= { espTransformEntry 11 }

esptRowStatus OBJECT-TYPE
SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other
objects in this conceptual row can be modified.

If active, this object must remain active if it is referenced
by a row in another table."
 ::= { espTransformEntry 12 }

--
-- IP compression transform definition table
--

```

ipcompTransformTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IpcompTransformEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table lists all the IP compression transforms which
         can be used to build IPsec proposals during negotiation of
         a phase 2 SA."
    ::= { ipsecPolicyConfigObjects 26 }

```

```

ipcompTransformEntry OBJECT-TYPE
    SYNTAX      IpcompTransformEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This entry contains the attributes of one IP compression
         transform."
    INDEX       { ipcompTransformName }
    ::= { ipcompTransformTable 1 }

```

```

IpcompTransformEntry ::= SEQUENCE {
    ipcompTransformName          SnmpAdminString,

```

```

    ipcompTransformMaxLifetimeSec      Unsigned32,
    ipcompTransformMaxLifetimeKB      Unsigned32,
    ipcompAlgorithm                    IpsecDoiIpcompTransform,
    ipcompDictionarySize               Unsigned32,
    ipcompPrivateAlgorithm             Unsigned32,
    ipcompTransformLastChanged         TimeStamp,
    ipcompTransformStorageType         StorageType,
    ipcompTransformRowStatus           RowStatus
}

```

```

ipcompTransformName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The name of this ipcompTransformEntry."
    ::= { ipcompTransformEntry 1 }

```

```

ipcompTransformMaxLifetimeSec OBJECT-TYPE

```


SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ipcompTransformMaxLifetimeSec specifies how long in seconds
the security association derived from this transform should be
used."
 ::= { ipcompTransformEntry 2 }

ipcompTransformMaxLifetimeKB OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ipcompTransformMaxLifetimeKB specifies how long in kilobytes
the security association derived from this transform should be
used."
 ::= { ipcompTransformEntry 3 }

ipcompAlgorithm OBJECT-TYPE

SYNTAX IsecDoiIpcompTransform
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ipcompAlgorithm specifies the transform ID of the IP compression
algorithm."
 ::= { ipcompTransformEntry 4 }

ipcompDictionarySize OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"If the algorithm in ipcompAlgorithm requires a dictionary
size configuration parameter, then this is the place to put
it. This object specifies the log2 maximum size of the
dictionary for the compression algorithm."
 ::= { ipcompTransformEntry 5 }

ipcompPrivateAlgorithm OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create
STATUS current
DESCRIPTION

"If ipcompPrivateAlgorithm has a value other zero, then it is up to the vendors implementation to determine the meaning of this field and substitute a data compression algorithm in place of ipcompAlgorithm."

::= { ipcompTransformEntry 6 }

ipcompTransformLastChanged OBJECT-TYPE

SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."

::= { ipcompTransformEntry 7 }

ipcompTransformStorageType OBJECT-TYPE

SYNTAX StorageType
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"The storage type for this row. Rows in this table which were created through an external process may have a storage type of readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

::= { ipcompTransformEntry 8 }

ipcompTransformRowStatus OBJECT-TYPE

SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the conceptual status of this row."

The value of this object has no effect on whether other objects in this conceptual row can be modified.

If active, this object must remain active if it is referenced by a row in another table."

```

 ::= { ipcompTransformEntry 9 }

--
-- IKE identity definition table
--

ikeIdentityTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IkeIdentityEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "IKEIdentity is used to represent the identities that may be
        used for an IPProtocolEndpoint (or collection of
        IPProtocolEndpoints) to identify itself in IKE phase 1
        negotiations.  The column ikeIdentityName in an
        ikeActionEntry together with the peEndpointIdentType and the
        peEndpointAddress in the PolicyEndpointToGroupTable specifies
        the unique identity to use in a negotiation exchange."
    ::= { ipsecPolicyConfigObjects 27 }

ikeIdentityEntry OBJECT-TYPE
    SYNTAX      IkeIdentityEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "ikeIdentity lists the attributes of an IKE identity."
    INDEX { peEndpointIdentType, peEndpointAddress,
            ikeIdentityType, ikeIdentityContext }
    ::= { ikeIdentityTable 1 }

IkeIdentityEntry ::= SEQUENCE {
    ikeIdValue          OCTET STRING,
    ikeIdKeyName        SnmpAdminString,
    ikeIdCredMngName    SnmpAdminString,
    ikeIdLastChanged    TimeStamp,
    ikeIdStorageType    StorageType,
    ikeIdRowStatus      RowStatus
}

ikeIdValue      OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..255))

```

MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ikeIdValue contains a string encoding of the Identity payload.
For IKEIdentity instances that are address types, the Identity
string value may be omitted and the associated
IPProtocolEndpoint or appropriate member of the Collection of
endpoints is used."
::= { ikeIdentityEntry 1 }

ikeIdKeyName OBJECT-TYPE
SYNTAX SnmpAdminString
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This value is used as an index into the keyTable to look up
the actual key value and other key information. For ID's
without associated keying information, this value is left
blank"
::= { ikeIdentityEntry 2 }

ikeIdCredMngName OBJECT-TYPE
SYNTAX SnmpAdminString
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This value is used as an index into the
ipsecCredMngServiceTable. For IDs that have no credential
management service, this value is left blank."
::= { ikeIdentityEntry 3 }

ikeIdLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or created
either through SNMP SETs or by some other external means."
::= { ikeIdentityEntry 4 }

ikeIdStorageType OBJECT-TYPE
SYNTAX StorageType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The storage type for this row. Rows in this table which were
created through an external process may have a storage type of
readOnly or permanent. Entries which are permanent are

Internet Draft

IPsec Policy Configuration MIB

June 2002

expected to have at least one configurable column in the row, but which columns are in fact modifiable is implementation specific."

```
DEFVAL { nonVolatile }
 ::= { ikeIdentityEntry 5 }
```

```
ikeIdRowStatus OBJECT-TYPE
```

```
SYNTAX      RowStatus
```

```
MAX-ACCESS  read-create
```

```
STATUS      current
```

```
DESCRIPTION
```

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other objects in this conceptual row can be modified.

If active, this object must remain active if it is referenced by a row in another table."

```
 ::= { ikeIdentityEntry 6 }
```

```
--
```

```
-- Peer Identity Table
```

```
--
```

```
peerIdentityTable OBJECT-TYPE
```

```
SYNTAX      SEQUENCE OF PeerIdentityEntry
```

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

```
STATUS      current
```

```
DESCRIPTION
```

"PeerIdentity is used to represent the identities that may be used for peers to identify themselves in IKE phase I/II negotiations. PeerIdentityTable aggregates the table entries that provide mappings between identities and their addresses."

```
 ::= { ipsecPolicyConfigObjects 28 }
```

```
peerIdentityEntry OBJECT-TYPE
```

```
SYNTAX      PeerIdentityEntry
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "peerIdentity matches a peer's identity to its address."
INDEX { peerIdName, peerIdPriority }
 ::= { peerIdentityTable 1 }
```

```
PeerIdentityEntry ::= SEQUENCE {
    peerIdName                               SnmpAdminString,
```

Various Authors

[Page 82]

Internet Draft

IPsec Policy Configuration MIB

June 2002

```
    peerIdPriority                           Integer32,
    peerIdValue                             OCTET STRING,
    peerIdType                              IsecDoiIdentType,
    peerIdAddress                          IsecIPAddress,
    peerIdAddressType                      IsecIPVersion,
    peerIdKeyName                          SnmpAdminString,
    peerIdCredMngName                      SnmpAdminString,
    peerIdLastChanged                      TimeStamp,
    peerIdStorageType                      StorageType,
    peerIdRowStatus                        RowStatus
}
```

peerIdName OBJECT-TYPE

```
SYNTAX      SnmpAdminString (SIZE(1..116))
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "This is an administratively assigned value that, together
    with peerIdPriority, uniquely identifies an entry in this table."
```

```
 ::= { peerIdentityEntry 1 }
```

peerIdPriority OBJECT-TYPE

```
SYNTAX      Integer32 (0..2147483647)
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "This object, along with peerIdName, uniquely identifies an entry in
    this table. The priority also indicates the order of peer gateways
    to initiate or accept SAs from (i.e. try until success)."
```

```
 ::= { peerIdentityEntry 2 }
```

peerIdValue OBJECT-TYPE

```
SYNTAX      OCTET STRING (SIZE(0..8192))
```

```
MAX-ACCESS read-create
```

```
STATUS      current
```

DESCRIPTION

"peerIdValue contains a string encoding of the Identity payload for the a peer."

::= { peerIdentityEntry 3 }

peerIdType OBJECT-TYPE
SYNTAX IpsecDoiIdentType
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"peerIdType is an enumeration identifying the type of the Identity value."

::= { peerIdentityEntry 4 }

peerIdAddress OBJECT-TYPE
SYNTAX IpsecIPAddress
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"The property PeerAddress specifies the IP address of the peer. The format is specified by the peerIdAddressType."

::= { peerIdentityEntry 5 }

peerIdAddressType OBJECT-TYPE
SYNTAX IpsecIPVersion
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"The property peerIdAddressType specifies the format of the peerIdAddress property value."

::= { peerIdentityEntry 6 }

peerIdKeyName OBJECT-TYPE
SYNTAX SnmpAdminString
MAX-ACCESS read-create
STATUS current

DESCRIPTION

"This value is used as an index into the keyTable to look up the actual key value and other key information. For peer IDs that have no associated key information, this value is left blank."

::= { peerIdentityEntry 7 }

peerIdCredMngName OBJECT-TYPE
SYNTAX SnmpAdminString
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This value is used as an index into the
ipsecCredMngServiceTable. For peer IDs that have no
credential management service, this value is left blank."
 ::= { peerIdentityEntry 8 }

peerIdLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or created
either through SNMP SETs or by some other external means."
 ::= { peerIdentityEntry 9 }

peerIdStorageType OBJECT-TYPE
SYNTAX StorageType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The storage type for this row. Rows in this table which were
created through an external process may have a storage type of
readOnly or permanent. Entries which are permanent are
expected to have at least one configurable column in the row, but
which columns are in fact modifiable is implementation specific."
DEFVAL { nonVolatile }
 ::= { peerIdentityEntry 10 }

peerIdRowStatus OBJECT-TYPE
SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other

objects in this conceptual row can be modified.

If active, this object must remain active if it is referenced by a row in another table."

```
::= { peerIdentityEntry 11 }
```

```
--
```

```
-- autostart IKE Table
```

```
--
```

```
autostartIkeTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF AutostartIkeEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"The parameters in the autostart IKE Table are used to automatically initiate IKE phases I and II (i.e. IPsec) negotiations at startup."
```

```
::= { ipsecPolicyConfigObjects 29 }
```

```
autostartIkeEntry OBJECT-TYPE
```

```
SYNTAX AutostartIkeEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

Various Authors

[Page 85]

Internet Draft

IPsec Policy Configuration MIB

June 2002

```
"autostart ike provides the set of parameters to automatically start IKE and IPsec SA's."
```

```
INDEX { autoIkePriority }
```

```
::= { autostartIkeTable 1 }
```

```
AutostartIkeEntry ::= SEQUENCE {
```

```
autoIkePriority
```

```
Integer32,
```

```
autoIkeAction
```

```
VariablePointer,
```

```
autoIkeAddressType
```

```
IpsecIPVersion,
```

```
autoIkeSourceAddress
```

```
IpsecIPAddress,
```

```
autoIkeSourcePort
```

```
Integer32,
```

```
autoIkeDestAddress
```

```
IpsecIPAddress,
```

```
autoIkeDestPort
```

```
Integer32,
```

```
autoIkeProtocol
```

```
Unsigned32,
```

```

    autoIkeLastChanged      TimeStamp,
    autoIkeStorageType      StorageType,
    autoIkeRowStatus        RowStatus
}

autoIkePriority OBJECT-TYPE
    SYNTAX      Integer32 (0..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "autoIkePriority is an index into the autostartIkeAction table
        and can be used to order the autostart IKE actions."
    ::= { autostartIkeEntry 1 }

autoIkeAction OBJECT-TYPE
    SYNTAX      VariablePointer
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This pointer is used to point to the action or compound action
        that should be initiated by this row."
    ::= { autostartIkeEntry 2 }

autoIkeAddressType OBJECT-TYPE
    SYNTAX      Ipv4Address
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The property autoIkeAddressType specifies the format of the
        autoIke source and destination Address values."
    ::= { autostartIkeEntry 3 }

autoIkeSourceAddress OBJECT-TYPE
    SYNTAX      IpsecIPAddress

```

```

    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The property autoIkeSourceAddress specifies Source IP address
        for autostarting IKE SA's, formatted according to the appropriate
        convention as defined in the autoIkeAddressType property."
    ::= { autostartIkeEntry 4 }

```

```

autoIkeSourcePort OBJECT-TYPE
    SYNTAX          Integer32
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The property autoIkeSourcePort specifies the port number for
         the source port for autotstarting IKE SA's."
    ::= { autostartIkeEntry 5 }

autoIkeDestAddress OBJECT-TYPE
    SYNTAX          IpsecIPAddress
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The property autoIkeDestAddress specifies the Destination IP
         address for autostarting IKE SA's, formatted according to the
         appropriate convention as defined in the autoIkeAddressType
         property."
    ::= { autostartIkeEntry 6 }

autoIkeDestPort OBJECT-TYPE
    SYNTAX          Integer32
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The property autoIkeDestPort specifies the port number for
         the destination port for autotstarting IKE SA's."
    ::= { autostartIkeEntry 7 }

autoIkeProtocol OBJECT-TYPE
    SYNTAX          Unsigned32 (0..255)
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The property Protocol specifies the protocol number used in
         comparing with policy filter entries and used in any phase 2
         negotiations."
    ::= { autostartIkeEntry 8 }

autoIkeLastChanged OBJECT-TYPE

```

SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The value of sysUpTime when this row was last modified or created
 either through SNMP SETs or by some other external means."
::= { autostartIkeEntry 9 }

autoIkeStorageType OBJECT-TYPE

SYNTAX StorageType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "The storage type for this row. Rows in this table which were
 created through an external process may have a storage type of
 readOnly or permanent. Entries which are permanent are
 expected to have at least one configurable column in the row, but
 which columns are in fact modifiable is implementation specific."
DEFVAL { nonVolatile }
::= { autostartIkeEntry 10 }

autoIkeRowStatus OBJECT-TYPE

SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "This object indicates the conceptual status of this row.

 The value of this object has no effect on whether other
 objects in this conceptual row can be modified."

::= { autostartIkeEntry 11 }

--
-- CA Table
--

ipsecCredMngServiceTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpsecCredMngServiceEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "A table of Credential Management Service values. This table is
 usually used for credential/certificate values that are used
 with a management service (e.g. Certificate Authorities)."
::= { ipsecPolicyConfigObjects 30 }

Internet Draft

IPsec Policy Configuration MIB

June 2002

ipsecCredMngServiceEntry OBJECT-TYPE

SYNTAX IpsecCredMngServiceEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A row in the ipsecCredMngServiceTable."

INDEX { icmsName }

::= { ipsecCredMngServiceTable 1 }

IpsecCredMngServiceEntry ::= SEQUENCE {

icmsName SnmpAdminString,

icmsPolicyStatement OCTET STRING,

icmsCRL OCTET STRING,

icmsCRLDistPoint OCTET STRING,

icmsDistinguishedName OCTET STRING,

icmsMaxChainLength Integer32,

icmsCRLRefreshFreq Integer32,

icmsValue OCTET STRING,

icmsLastChanged TimeStamp,

icmsStorageType StorageType,

icmsRowStatus RowStatus

}

icmsName OBJECT-TYPE

SYNTAX SnmpAdminString(SIZE(1..117))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This is an administratively assigned string used to index
this table."

::= { ipsecCredMngServiceEntry 1 }

icmsPolicyStatement OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..8192))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This Value represents the Credential Management Service
Policy Statement, or a reference describing how to obtain it
(e.g., a URL). If one doesn't exist, this value can be left
blank"

::= { ipsecCredMngServiceEntry 2 }

icmsCRL OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..8192))
MAX-ACCESS read-create
STATUS current
DESCRIPTION

Various Authors

[Page 89]

Internet Draft

IPsec Policy Configuration MIB

June 2002

"This value is the CRL for this Credential Management Service."
 ::= { ipsecCredMngServiceEntry 3 }

icmsCRLDistPoint OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..8192))
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This value represents the CRL Distribution Point for the Credential Management Service."
 ::= { ipsecCredMngServiceEntry 4 }

icmsDistinguishedName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..8192))
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This value represents the Distinguished Name of the Credential Management Service."
 ::= { ipsecCredMngServiceEntry 5 }

icmsMaxChainLength OBJECT-TYPE
SYNTAX Integer32 (0..255)
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This value is the maximum length of the chain allowable from the Credential Management Service to the credential in question."
 DEFVAL { 0 }
 ::= { ipsecCredMngServiceEntry 6 }

icmsCRLRefreshFreq OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-create

STATUS current
DESCRIPTION
"This value is the refresh frequency in seconds."
 ::= { ipsecCredMngServiceEntry 7 }

icmsValue OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..8192))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This is the actual certificate value (i.e. key) for this
Credential Management Service."

Various Authors

[Page 90]

Internet Draft

IPsec Policy Configuration MIB

June 2002

::= { ipsecCredMngServiceEntry 8 }

icmsLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or created
either through SNMP SETs or by some other external means."
 ::= { ipsecCredMngServiceEntry 9 }

icmsStorageType OBJECT-TYPE
SYNTAX StorageType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The storage type for this row. Rows in this table which were
created through an external process may have a storage type of
readOnly or permanent. Entries which are permanent are
expected to have at least one configurable column in the row, but
which columns are in fact modifiable is implementation specific."
 ::= { ipsecCredMngServiceEntry 10 }

icmsRowStatus OBJECT-TYPE
SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object indicates the conceptual status of this row."

The value of this object has no effect on whether other objects in this conceptual row can be modified.

If active, this object must remain active if it is referenced by a row in another table."

::= { ipsecCredMngServiceEntry 11 }

--
-- Key Table
--

keyTable OBJECT-TYPE
SYNTAX SEQUENCE OF KeyEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

Various Authors

[Page 91]

Internet Draft

IPsec Policy Configuration MIB

June 2002

"A table of key values. Among other uses, this table can be used for keying information for preconfigured IPsec actions."

::= { ipsecPolicyConfigObjects 31 }

keyEntry OBJECT-TYPE
SYNTAX KeyEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"A row in the keyTable."
INDEX { ktName }
::= { keyTable 1 }

KeyEntry ::= SEQUENCE {
 ktName SnmpAdminString,
 ktRemoteID OCTET STRING,
 ktKey OCTET STRING,
 ktPasswordAlgorithm OCTET STRING,
 ktLastChanged TimeStamp,
 ktStorageType StorageType,
 ktRowStatus RowStatus

}

ktName OBJECT-TYPE

SYNTAX SnmpAdminString(SIZE(1..32))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This object represents the name for an entry in this table."

::= { keyEntry 1 }

ktRemoteID OBJECT-TYPE

SYNTAX OCTET STRING(SIZE(0..256))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object represents the Identification (e.g. user name) of the user of the key information on the remote site. If there is no ID associated with this key, the value of this object should be the null string."

::= { keyEntry 2 }

ktKey OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..4096))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object represents the key value. When accessed for reading, it MUST return a null length (0 length) string and MUST NOT return the configured key."

::= { keyEntry 3 }

ktPasswordAlgorithm OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..4096))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object represents the transformation algorithm used to protect passwords before use in the protocol. For shared keys without a password, this value can be ignored. For shared keys that have passwords but no transform algorithm, this object should be the null string."

```
::= { keyEntry 4 }
```

```
ktLastChanged OBJECT-TYPE
```

```
SYNTAX TimeStamp
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"The value of sysUpTime when this row was last modified or created  
either through SNMP SETs or by some other external means."
```

```
::= { keyEntry 5 }
```

```
ktStorageType OBJECT-TYPE
```

```
SYNTAX StorageType
```

```
MAX-ACCESS read-create
```

```
STATUS current
```

```
DESCRIPTION
```

```
"The storage type for this row. Rows in this table which were  
created through an external process may have a storage type of  
readOnly or permanent. Entries which are permanent are  
expected to have at least one configurable column in the row, but  
which columns are in fact modifiable is implementation specific."
```

```
::= { keyEntry 6 }
```

```
ktRowStatus OBJECT-TYPE
```

```
SYNTAX RowStatus
```

```
MAX-ACCESS read-create
```

```
STATUS current
```

```
DESCRIPTION
```

```
"This object indicates the conceptual status of this row.
```

```
The value of this object has no effect on whether other  
objects in this conceptual row can be modified.
```

```
If active, this object must remain active if it is referenced  
by a row in another table."
```

```
::= { keyEntry 7 }
```

```
--
```

```
--
```

```
-- Notification objects information
```

```
--
```

--

```
ipsecPolicyNotificationVariables OBJECT IDENTIFIER ::=
  { ipsecPolicyNotificationObjects 1 }
```

```
ipsecPolicyNotifications OBJECT IDENTIFIER ::=
  { ipsecPolicyNotificationObjects 0 }
```

```
ipsecPolicyActionExecuted OBJECT-TYPE
  SYNTAX      VariablePointer
  MAX-ACCESS  accessible-for-notify
  STATUS      current
  DESCRIPTION
    "Points to the action instance that was executed that
     resulted in the notification being sent."
  ::= { ipsecPolicyNotificationVariables 1 }
```

```
ipsecPolicyActionSource OBJECT-TYPE
  SYNTAX      VariablePointer
  MAX-ACCESS  accessible-for-notify
  STATUS      current
  DESCRIPTION
    "Contains the source address of the packet which triggered the
     action in question."
  ::= { ipsecPolicyNotificationVariables 2 }
```

```
ipsecPolicyActionDestination OBJECT-TYPE
  SYNTAX      VariablePointer
  MAX-ACCESS  accessible-for-notify
  STATUS      current
  DESCRIPTION
    "Contains the destination address of the packet which triggered the
     action in question."
  ::= { ipsecPolicyNotificationVariables 3 }
```

```
ipsecPolicyPacketDirection OBJECT-TYPE
  SYNTAX      INTEGER { inbound(1), outbound(2) }
  MAX-ACCESS  accessible-for-notify
  STATUS      current
  DESCRIPTION
```

```

        was inbound our outbound."
 ::= { ipsecPolicyNotificationVariables 4 }

ipsecPolicyActionNotification NOTIFICATION-TYPE
  OBJECTS { ipsecPolicyActionExecuted,
            ipsecPolicyActionSource, ipsecPolicyActionDestination,
            peGroupName, ipsecPolicyPacketDirection }
  STATUS current
  DESCRIPTION
    "Notification that a action was executed by a rule. Only
    actions with logging enabled will result in this notification
    getting sent. The objects sent must include the pRuleType
    object, which will indicate which rule activated the action
    and what type of rule it was, as well as the
    ipsecPolicyActionExecuted object which will indicate which
    action was executed within the scope of the rule.
    Additionally the ipsecPolicyActionSource,
    ipsecPolicyActionDestination objects must be included to
    indicate the packet source and destination of the packet that
    triggered the action. Finally, the peGroupName and
    ipsecPolicyPacketDirection objects are included to indicate
    which endpoint the action was executed in association with
    and if the inbound or outbond through the endpoint.

    Note that compound actions with multiple
    executed subactions may result in multiple notifications
    being sent from a single rule execution."
 ::= { ipsecPolicyNotifications 1 }

--
--
-- Conformance information
--
--

ipsecPolicyCompliances OBJECT IDENTIFIER ::=
                                { ipsecPolicyConformanceObjects 1 }
ipsecPolicyGroups OBJECT IDENTIFIER ::=
                                { ipsecPolicyConformanceObjects 2 }

--
-- Compliance statements
--
--

ipsecPolicyRuleFilterCompliance MODULE-COMPLIANCE
  STATUS current

```

DESCRIPTION

"The compliance statement for SNMP entities that include an IPsec MIB implementation with Endpoint, Rules, and filters support."

MODULE -- This Module

```
MANDATORY-GROUPS { ipsecPolicyEndpointGroup,
                    ipsecPolicyGroupContentsGroup,
                    ipsecPolicyRuleDefinitionGroup,
                    ipsecPolicyIPHeaderFilterGroup,
                    ipsecPolicyStaticFilterGroup }
```

GROUP ipsecSystemPolicyNameGroup

DESCRIPTION

"This group is mandatory for IPsec Policy implementations which support a system policy group name."

GROUP ipsecPolicyCompoundFilterGroup

DESCRIPTION

"This group is mandatory for IPsec Policy implementations which support compound filters."

GROUP ipsecPolicyTimeFilterGroup

DESCRIPTION

"This group is mandatory for IPsec Policy implementations which support time filters."

GROUP ipsecPolicyIpsHeaderFilterGroup

DESCRIPTION

"This group is mandatory for IPsec Policy implementations which support IPSO Header filters."

GROUP ipsecPolicyCredentialFilterGroup

DESCRIPTION

"This group is mandatory for IPsec Policy implementations which support Credential filters."

GROUP ipsecPolicyPeerIdFilterGroup

DESCRIPTION

"This group is mandatory for IPsec Policy implementations which support Peer Identity filters."

OBJECT peRowStatus

SYNTAX INTEGER {

active(1), createAndGo(4), destroy(6)

}

DESCRIPTION

"Support of the values notInService(2), notReady(3),

and createAndWait(5) is not required."

OBJECT peLastChanged
MIN-ACCESS not-accessible
DESCRIPTION

"This object not required for compliance."

OBJECT pgcGroupComponentType
SYNTAX INTEGER {
rule(2)
}

DESCRIPTION

"Support of the value group(1) is only required for implementations which support Policy Groups within Policy Groups."

OBJECT pgcRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}

DESCRIPTION

"Support of the values notInService(2), notReady(3), and createAndWait(5) is not required."

OBJECT pgcLastChanged
MIN-ACCESS not-accessible
DESCRIPTION

"This object not required for compliance."

OBJECT pRuleRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}

DESCRIPTION

"Support of the values notInService(2), notReady(3), and createAndWait(5) is not required."

OBJECT pRuleLastChanged
MIN-ACCESS not-accessible

DESCRIPTION
"This object not required for compliance."

OBJECT cfRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}

DESCRIPTION
"Support of the values notInService(2), notReady(3),

Various Authors

[Page 97]

Internet Draft

IPsec Policy Configuration MIB

June 2002

and createAndWait(5) is not required."

OBJECT cfLastChanged
MIN-ACCESS not-accessible
DESCRIPTION

"This object not required for compliance."

OBJECT ficRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}

DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT ficLastChanged
MIN-ACCESS not-accessible
DESCRIPTION

"This object not required for compliance."

OBJECT ihfRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}

DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT ihfLastChanged
MIN-ACCESS not-accessible
DESCRIPTION

"This object not required for compliance."

OBJECT tfRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT tfLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object not required for compliance."

OBJECT ipsohfRowStatus
SYNTAX INTEGER {

active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT ipsohfLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object not required for compliance."

OBJECT crfRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT crfLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object not required for compliance."

OBJECT pifRowStatus


```

SYNTAX      INTEGER {
                active(1), createAndGo(4), destroy(6)
            }
DESCRIPTION
    "Support of the values notInService(2), notReady(3),
    and createAndWait(5) is not required."

OBJECT      pifLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object not required for compliance."

OBJECT      icmsRowStatus
SYNTAX      INTEGER {
                active(1), createAndGo(4), destroy(6)
            }
DESCRIPTION
    "Support of the values notInService(2), notReady(3),
    and createAndWait(5) is not required."

OBJECT      icmsLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION

```

"This object not required for compliance."

```
 ::= { ipsecPolicyCompliances 1 }
```

```

ipsecPolicyIPsecCompliance MODULE-COMPLIANCE
STATUS      current
DESCRIPTION
    "The compliance statement for SNMP entities that include an
    IPsec MIB implementation and supports IPsec actions."
MODULE -- This Module
MANDATORY-GROUPS { ipsecPolicyIpsecGroup,
                    ipsecPolicyStaticActionGroup,
                    ipsecPolicyPreconfiguredGroup }

GROUP ipsecPolicyCompoundActionGroup
DESCRIPTION
    "This group is mandatory for IPsec Policy

```

implementations which support compound actions."

OBJECT caRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT caLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT aicaRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT aicaLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT ipsecActionRowStatus
SYNTAX INTEGER {

active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT ipsecActionLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT ipsecProposalsRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT ipsecProposalsLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT ipsecTransformsRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT ipsecTransformsLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT sanRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT sanLastChanged
MIN-ACCESS not-accessible
DESCRIPTION

"This object is not required for compliance."

OBJECT ahtRowStatus
SYNTAX INTEGER {

```

        active(1), createAndGo(4), destroy(6)
    }
DESCRIPTION
    "Support of the values notInService(2), notReady(3),
    and createAndWait(5) is not required."

OBJECT      ahtLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is not required for compliance."

OBJECT      esptRowStatus
SYNTAX      INTEGER {
        active(1), createAndGo(4), destroy(6)
    }
DESCRIPTION
    "Support of the values notInService(2), notReady(3),
    and createAndWait(5) is not required."

OBJECT      esptLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is not required for compliance."

OBJECT      ipcompTransformRowStatus
SYNTAX      INTEGER {
        active(1), createAndGo(4), destroy(6)
    }
DESCRIPTION
    "Support of the values notInService(2), notReady(3),
    and createAndWait(5) is not required."

OBJECT      ipcompTransformLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is not required for compliance."

OBJECT      peerIdRowStatus
SYNTAX      INTEGER {
        active(1), createAndGo(4), destroy(6)
    }
DESCRIPTION
    "Support of the values notInService(2), notReady(3),
    and createAndWait(5) is not required."

```

OBJECT peerIdLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT icmsRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT icmsLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object not required for compliance."

OBJECT ktRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT ktLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT sapRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT sapLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

::= { ipsecPolicyCompliances 2 }

ipsecPolicyIKECompliance MODULE-COMPLIANCE

DESCRIPTION

"The compliance statement for SNMP entities that include an IPsec MIB implementation and supports IKE actions."

MODULE -- This Module

MANDATORY-GROUPS { ipsecPolicyIkeGroup }

GROUP ipsecPolicyCompoundActionGroup

DESCRIPTION

"This group is mandatory for IPsec Policy implementations which support compound actions."

OBJECT caRowStatus

SYNTAX INTEGER {

active(1), createAndGo(4), destroy(6)

}

DESCRIPTION

"Support of the values notInService(2), notReady(3), and createAndWait(5) is not required."

OBJECT caLastChanged

MIN-ACCESS not-accessible

DESCRIPTION

"This object is not required for compliance."

OBJECT aicaRowStatus

SYNTAX INTEGER {

active(1), createAndGo(4), destroy(6)

}

DESCRIPTION

"Support of the values notInService(2), notReady(3), and createAndWait(5) is not required."

OBJECT aicaLastChanged

MIN-ACCESS not-accessible

DESCRIPTION

"This object is not required for compliance."

OBJECT ikeActionRowStatus

SYNTAX INTEGER {

active(1), createAndGo(4), destroy(6)

```
}
DESCRIPTION
    "Support of the values notInService(2), notReady(3),
    and createAndWait(5) is not required."
```

```
OBJECT      ikeActionLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
```

Various Authors

[Page 104]

Internet Draft

IPsec Policy Configuration MIB

June 2002

"This object is not required for compliance."

```
OBJECT      ikeActionProposalRowStatus
SYNTAX      INTEGER {
    active(1), createAndGo(4), destroy(6)
}
```

```
DESCRIPTION
    "Support of the values notInService(2), notReady(3),
    and createAndWait(5) is not required."
```

```
OBJECT      ikeActionProposalLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
```

"This object is not required for compliance."

```
OBJECT      ipProposalRowStatus
SYNTAX      INTEGER {
    active(1), createAndGo(4), destroy(6)
}
```

```
DESCRIPTION
    "Support of the values notInService(2), notReady(3),
    and createAndWait(5) is not required."
```

```
OBJECT      ipProposalLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
```

"This object is not required for compliance."

```
OBJECT      sanRowStatus
SYNTAX      INTEGER {
    active(1), createAndGo(4), destroy(6)
}
```

```
DESCRIPTION
```

"Support of the values notInService(2), notReady(3), and createAndWait(5) is not required."

OBJECT sanLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT ikeIdRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3), and createAndWait(5) is not required."

OBJECT ikeIdLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT peerIdRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3), and createAndWait(5) is not required."

OBJECT peerIdLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT icmsRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3), and createAndWait(5) is not required."

OBJECT icmsLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object not required for compliance."

OBJECT autoIkeRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}
DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT autoIkeLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

OBJECT ktRowStatus
SYNTAX INTEGER {
active(1), createAndGo(4), destroy(6)
}

DESCRIPTION
"Support of the values notInService(2), notReady(3),
and createAndWait(5) is not required."

OBJECT ktLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
"This object is not required for compliance."

::= { ipsecPolicyCompliances 3 }

policyLoggingCompliance MODULE-COMPLIANCE

STATUS current

DESCRIPTION

"The compliance statement for SNMP entities that support
sending notifications when actions are invoked."

MODULE -- This Module

MANDATORY-GROUPS { policyActionLoggingObjectGroup,
policyActionNotificationGroup }

```

 ::= { ipsecPolicyCompliances 4 }

--
--
-- Compliance Groups Definitions
--
--
--
-- Endpoint, Rule, Filter Compliance Groups
--

ipsecPolicyEndpointGroup OBJECT-GROUP
  OBJECTS {
    peGroupName, peLastChanged, peStorageType, peRowStatus
  }
  STATUS current
  DESCRIPTION
    "The IPsec Policy Endpoint Table Group."
  ::= { ipsecPolicyGroups 1 }

ipsecPolicyGroupContentsGroup OBJECT-GROUP
  OBJECTS {
    pgcGroupComponentType, pgcFilter, pgcGroupComponentName,
    pgcLastChanged, pgcStorageType, pgcRowStatus
  }
  STATUS current
  DESCRIPTION

```

```

    "The IPsec Policy Group Contents Table Group."
  ::= { ipsecPolicyGroups 2 }

ipsecSystemPolicyNameGroup OBJECT-GROUP
  OBJECTS {
    systemPolicyGroupName
  }
  STATUS current
  DESCRIPTION
    "The System Policy Group Name Group."
  ::= { ipsecPolicyGroups 3}

```

```

ipsecPolicyRuleDefinitionGroup OBJECT-GROUP
  OBJECTS {
    pRuleDescription, pRuleFilter,
    pRuleFilterNegated, pRuleAction, pRuleAdminStatus,
    pRuleLastChanged, pRuleStorageType,
    pRuleRowStatus
  }
  STATUS current
  DESCRIPTION
    "The IPsec Policy Rule Definition Table Group."
  ::= { ipsecPolicyGroups 4 }

```

```

ipsecPolicyCompoundFilterGroup OBJECT-GROUP
  OBJECTS {
    cfDescription, cfLogicType, cfLastChanged, cfStorageType,
    cfRowStatus, ficSubfilter, ficSubfilterIsNegated,
    ficLastChanged, ficStorageType, ficRowStatus
  }
  STATUS current
  DESCRIPTION
    "The IPsec Policy Compound Filter Table and Filters in
    Compound Filters Table Group."
  ::= { ipsecPolicyGroups 5 }

```

```

ipsecPolicyStaticFilterGroup OBJECT-GROUP
  OBJECTS { trueFilter, ikePhase1Filter, ikePhase2Filter }
  STATUS current
  DESCRIPTION
    "The static filter group. Currently this is just a true
    filter."
  ::= { ipsecPolicyGroups 6 }

```

```

ipsecPolicyIPHeaderFilterGroup OBJECT-GROUP
  OBJECTS {
    ihfType, ihfIPVersion, ihfSrcAddressBegin, ihfSrcAddressEnd,
    ihfDstAddressBegin, ihfDstAddressEnd, ihfSrcLowPort,

```

```

    ihfSrcHighPort, ihfDstLowPort, ihfDstHighPort, ihfProtocol,
    ihfIPv6FlowLabel, ihfLastChanged, ihfStorageType, ihfRowStatus
  }
  STATUS current
  DESCRIPTION

```

```

    "The IPsec Policy IP Header Filter Table Group."
 ::= { ipsecPolicyGroups 7 }

ipsecPolicyTimeFilterGroup OBJECT-GROUP
OBJECTS {
    tfPeriodStart, tfPeriodEnd, tfMonthOfYearMask,
    tfDayOfMonthMask, tfDayOfWeekMask, tfTimeOfDayMaskStart,
    tfTimeOfDayMaskEnd, tfLastChanged, tfStorageType, tfRowStatus
}
STATUS current
DESCRIPTION
    "The IPsec Policy Time Filter Table Group."
 ::= { ipsecPolicyGroups 8 }

ipsecPolicyIpsHeaderFilterGroup OBJECT-GROUP
OBJECTS {
    ipsohfType, ipsohfClassification, ipsohfProtectionAuth,
    ipsohfLastChanged, ipsohfStorageType, ipsohfRowStatus
}
STATUS current
DESCRIPTION
    "The IPsec Policy IPSO Header Filter Table Group."
 ::= { ipsecPolicyGroups 9 }

ipsecPolicyCredentialFilterGroup OBJECT-GROUP
OBJECTS {
    crfCredentialType, crfMatchFieldName, crfMatchFieldValue,
    crfAcceptCredFrom, crfLastChanged, crfStorageType,
    crfRowStatus,

    icmsPolicyStatement, icmsCRL, icmsCRLDistPoint,
    icmsDistinguishedName, icmsMaxChainLength,
    icmsCRLRefreshFreq, icmsValue, icmsLastChanged,
    icmsStorageType, icmsRowStatus
}
STATUS current
DESCRIPTION
    "The IPsec Policy Credential Filter Table Group."
 ::= { ipsecPolicyGroups 10 }

ipsecPolicyPeerIdFilterGroup OBJECT-GROUP
OBJECTS {
    pifIdentityType, pifIdentityValue,

```

```

        pifLastChanged, pifStorageType, pifRowStatus
    }
    STATUS current
    DESCRIPTION
        "The IPsec Policy Peer Identity Filter Table Group."
    ::= { ipsecPolicyGroups 11 }

--
-- action compliance groups
--

ipsecPolicyCompoundActionGroup OBJECT-GROUP
    OBJECTS {
        caExecutionStrategy, caLastChanged, caStorageType,
        caRowStatus, aicaSubActionName, aicaLastChanged,
        aicaStorageType, aicaRowStatus
    }
    STATUS current
    DESCRIPTION
        "The IPsec Policy Compound Action Table and Actions In
        Compound Action Table Group."
    ::= { ipsecPolicyGroups 12 }

ipsecPolicyPreconfiguredGroup OBJECT-GROUP
    OBJECTS {
        sapActionDescription,
        sapActionLifetimeSec, sapActionLifetimeKB, sapDoActionLogging,
        sapDoPacketLogging, sapDFHandling, sapActionType, sapAHSPI,
        sapAHTransformName, sapAHSharedSecretName, sapESPSPI,
        sapESPTransformName, sapESPEncSharedSecretName,
        sapESPAuthSharedSecretName, sapIPCompSPI,
        sapIPCompTransformName, sapPeerGatewayIdName,
        sapLastChanged, sapStorageType, sapRowStatus,

        ahtMaxLifetimeSec, ahtMaxLifetimeKB, ahtAlgorithm,
        ahtReplayProtection, ahtReplayWindowSize, ahtLastChanged,
        ahtStorageType,

        esptMaxLifetimeSec, esptMaxLifetimeKB,
        esptCipherTransformId, esptCipherKeyLength,
        esptCipherKeyRounds, esptIntegrityAlgorithmId,
        esptReplayPrevention, esptReplayWindowSize,
        esptLastChanged, esptStorageType, esptRowStatus,

        ipcompDictionarySize, ipcompTransformMaxLifetimeSec,
        ipcompTransformMaxLifetimeKB, ipcompPrivateAlgorithm,
        ipcompTransformLastChanged, ipcompTransformStorageType,
        ipcompTransformRowStatus,

```

Internet Draft

IPsec Policy Configuration MIB

June 2002

```
peerIdValue, peerIdType, peerIdAddress, peerIdAddressType,
peerIdKeyName, peerIdCredMngName, peerIdLastChanged,
peerIdStorageType, peerIdRowStatus,
```

```
icmsPolicyStatement, icmsCRL, icmsCRLDistPoint,
icmsDistinguishedName, icmsMaxChainLength,
icmsCRLRefreshFreq, icmsValue, icmsLastChanged,
icmsStorageType, icmsRowStatus,
```

```
ktRemoteID, ktKey, ktPasswordAlgorithm,
ktLastChanged, ktStorageType, ktRowStatus
```

}

STATUS current

DESCRIPTION

```
"This group is the set of objects that support preconfigured
IPsec actions. These objects are from The Preconfigured
Action Table. This group also includes objects from the
shared tables: Peer Identity Table, Key Table, Credential
Management Service Table and the AH, ESP, and IPComp
Transform Tables."
```

::= { ipsecPolicyGroups 13 }

ipsecPolicyStaticActionGroup OBJECT-GROUP

OBJECTS {

```
saDropAction, saAcceptAction, saRejectIKEAction,
saDropActionLog, saAcceptActionLog, saRejectIKEActionLog
```

}

STATUS current

DESCRIPTION

```
"The IPsec Policy Static Actions Group."
```

::= { ipsecPolicyGroups 14 }

ipsecPolicyIpsecGroup OBJECT-GROUP

OBJECTS {

```
ipsecActionParametersName, ipsecActionProposalsName,
ipsecUsePfs, ipsecVendorId, ipsecGroupId,
ipsecPeerGatewayIdName, ipsecUseIkeGroup, ipsecGranularity,
ipsecMode, ipsecDFHandling, ipsecDoActionLogging,
ipsecDoPacketLogging, ipsecActionLastChanged,
ipsecActionStorageType, ipsecActionRowStatus,
```

```
ipsecProposalsTransformsName, ipsecProposalsLastChanged,
```

ipsecProposalsStorageType, ipsecProposalsRowStatus,
ipsecTransformsTransformName, ipsecTransformsLastChanged,
ipsecTransformsStorageType, ipsecTransformsRowStatus,
sanMinimumLifetimeSeconds, sanMinimumLifetimeKB,

sanRefreshThresholdSeconds, sanRefreshThresholdKB,
sanIdleDurationSeconds, sanLastChanged, sanStorageType,
sanRowStatus,

ahtMaxLifetimeSec, ahtMaxLifetimeKB, ahtAlgorithm,
ahtReplayProtection, ahtReplayWindowSize, ahtLastChanged,
ahtStorageType, ahtRowStatus,

esptMaxLifetimeSec, esptMaxLifetimeKB,
esptCipherTransformId, esptCipherKeyLength,
esptCipherKeyRounds, esptIntegrityAlgorithmId,
esptReplayPrevention, esptReplayWindowSize,
esptLastChanged, esptStorageType, esptRowStatus,

ipcompDictionarySize, ipcompAlgorithm,
ipcompTransformMaxLifetimeSec, ipcompTransformMaxLifetimeKB,
ipcompPrivateAlgorithm, ipcompTransformLastChanged,
ipcompTransformStorageType, ipcompTransformRowStatus,

peerIdValue, peerIdType, peerIdAddress, peerIdAddressType,
peerIdKeyName, peerIdCredMngName, peerIdLastChanged,
peerIdStorageType, peerIdRowStatus,

icmsPolicyStatement, icmsCRL, icmsCRLDistPoint,
icmsDistinguishedName, icmsMaxChainLength,
icmsCRLRefreshFreq, icmsValue, icmsLastChanged,
icmsStorageType, icmsRowStatus,

ktRemoteID, ktKey, ktPasswordAlgorithm,
ktLastChanged, ktStorageType, ktRowStatus

}

STATUS current

DESCRIPTION

"This group is the set of objects that support IPsec
actions. These objects are from The IPsec Policy IPsec

Actions Table, The IPsec Proposal Table, and The IPsec Transform Table. This group also includes objects from the shared tables: Peer Identity Table, Key Table, Negotiation Parameters Table, Credential Management Service Table and the AH, ESP, and IPComp Transform Table."

```
::= { ipsecPolicyGroups 15 }
```

```
ipsecPolicyIkeGroup OBJECT-GROUP
```

```
OBJECTS {
```

```
    ikeActionParametersName, ikeThresholdDerivedKeys,  
    ikeExchangeMode, ikeAgressiveModeGroupId, ikeIdentityType,  
    ikeIdentityContext, ikePeerName, ikeActionVendorId,  
    ikeActionProposalName, ikeActionDoActionLogging,
```

Various Authors

[Page 112]

Internet Draft

IPsec Policy Configuration MIB

June 2002

```
    ikeActionDoPacketLogging, ikeActionLastChanged,  
    ikeActionStorageType, ikeActionRowStatus,
```

```
    ikeActionProposalLastChanged, ikeActionProposalStorageType,  
    ikeActionProposalRowStatus,
```

```
    ipLifetimeDerivedKeys, ipCipherAlgorithm, ipCipherKeyLength,  
    ipCipherKeyRounds, ipHashAlgorithm, ipPrfAlgorithm,  
    ipVendorId, ipDhGroup, ipAuthenticationMethod,  
    ipMaxLifetimeSeconds, ipMaxLifetimeKB,  
    ipProposalLastChanged, ipProposalStorageType,  
    ipProposalRowStatus,
```

```
    sanMinimumLifetimeSeconds, sanMinimumLifetimeKB,  
    sanRefreshThresholdSeconds, sanRefreshThresholdKB,  
    sanIdleDurationSeconds, sanLastChanged, sanStorageType,  
    sanRowStatus,
```

```
    ikeIdValue, ikeIdKeyName, ikeIdCredMngName, ikeIdLastChanged,  
    ikeIdStorageType, ikeIdRowStatus,
```

```
    autoIkeAction, autoIkeAddressType, autoIkeSourceAddress,  
    autoIkeSourcePort, autoIkeDestAddress, autoIkeDestPort,  
    autoIkeProtocol, autoIkeLastChanged, autoIkeStorageType,  
    autoIkeRowStatus,
```

```
    peerIdValue, peerIdType, peerIdAddress, peerIdAddressType,  
    peerIdKeyName, peerIdCredMngName, peerIdLastChanged,
```



```

peerIdStorageType, peerIdRowStatus,

icmsPolicyStatement, icmsCRL, icmsCRLDistPoint,
icmsDistinguishedName, icmsMaxChainLength,
icmsCRLRefreshFreq, icmsValue, icmsLastChanged,
icmsStorageType, icmsRowStatus,

ktRemoteID, ktKey, ktPasswordAlgorithm,
ktLastChanged, ktStorageType, ktRowStatus
}
STATUS current
DESCRIPTION
  "This group is the set of objects that support IKE
  actions. These objects are from The IPsec Policy IKE Action
  Table, The IKE Action Proposals Table, The IKE Proposal
  Table, The autostart IKE Table and The IKE Identity Table
  . This group also includes objects from the shared tables:
  Peer Identity Table, Credential Management Service Table and
  Negotiation Parameters Table."
 ::= { ipsecPolicyGroups 16 }

```

```

policyActionLoggingObjectGroup OBJECT-GROUP
  OBJECTS {
    ipsecPolicyActionExecuted, ipsecPolicyActionSource,
    ipsecPolicyActionDestination, ipsecPolicyPacketDirection
  }
  STATUS current
  DESCRIPTION
    "Notification objects."
  ::= { ipsecPolicyGroups 17 }

```

```

policyActionNotificationGroup NOTIFICATION-GROUP
  NOTIFICATIONS {
    ipsecPolicyActionNotification
  }
  STATUS current
  DESCRIPTION
    "Notifications."
  ::= { ipsecPolicyGroups 18 }

```

END

5. Security Considerations

5.1. Introduction

This document defines an SNMP MIB used to configure IPsec services. Since IPsec provides security services it is important that the IPsec configuration data be at least as protected as the IPsec provided security service. There are two threat you need to thwart when configuring IPsec devices.

1) only authentic administrators should be allowed to configure devices. 2) unfriendly parties should not be able to read configuration data while the data is in network transit.

SNMP version 3 provide security services. Therefore, when configuring data in the IPSEC-POLICY-MIB, you SHOULD use SNMP version 3. The rest of this discussion assumes the use of SNMPv3.

SNMPv3 has security services built into the protocol. This is a real strength, because it allows administrators the ability to load new IPsec configuration on a device and keep the conversation private and authenticated under the protection of SNMPv3 before any IPsec protections are available. Once you do establish some IPsec configuration on your device, it would be possible to set up IPsec SAs to then also provide security and integrity services to the

configuration conversation. This may seem redundant at first, but will be shown to have a use for added privacy protection below.

5.2. Protecting against in-authentic access

The current SNMPv3 User Security Model provides for key based user authentication. Typically, keys are derived from passwords (but are not required to be), and the keys are then used in HMAC algorithms (currently MD5 and SHA-1 HMACs are defined) to authenticate all SNMP data. Each SNMP device keeps a (configured) list of users and keys. Under SNMPv3 user keys may be updated as often as an administrator cares to have users enter new passwords. But Perfect Forward Secrecy for user keys is not yet provided by standards track documents, although [RFC2786](#) defines an experimental method of doing so.

SNMPv3 also provides a View Based Access Model. Different users may be given different levels of access (read-write, read-only...) to lists of SNMP objects or subtrees. This view based access control provides fine levels of access control granularity, making it possible to allow some administrators to have control over certain sections of this MIB will prohibiting them from accessing and/or modifying other sections of the MIB. This may be useful if local policy administrators should be given rights to add or amend certain policies, but should not be given rights to change, for example, corporate level policies.

[5.3.](#) Protecting against involuntary disclosure

While sending IPsec configuration data to a PEP, there are a few critical parameters which MUST NOT be observed by third parties. These include IKE Pre-Shared Keys and possibly the private key of a public/private key pair for use in a PKI. Were either of those parameters to be known to a third party, they could then impersonate your device to other IKE peers. And aside from those critical parameters, policy administrators may have an interest in not divulging their any of their policy configuration. SNMPv3 offers privacy security services, but at the time this document was written, it only supported the DES algorithm for privacy services. Support for other (stronger) crypto algorithms was in the works and may be done as you read this. Policy administrators SHOULD use a privacy security service to configure their IPsec policy which is at least as strong as the desired IPsec policy. It is unwise to configure IPsec parameters implementing 3DES algorithms while protecting that conversation with single DES.

[5.4.](#) Bootstrapping your configuration

Hopefully vendors will not ship new products with a default SNMPv3

user/password pair, but it is possible. Most SNMPv3 distributions should hopefully require an out-of-band initialization over a trusted medium, such as a local console connection.

[6.](#) Authors' Addresses:

Michael Baer

Network Associates, Inc.
3965 Freedom Circle, Suite 500
Santa Clara, CA 95054
Phone: +1 530 304 1628
Email: mike_baer@nai.com

Ricky Charlet
Email: rcharlet@alumni.calpoly.edu

Wes Hardaker
Network Associates, Inc.
3965 Freedom Circle, Suite 500
Santa Clara, CA 95054
Phone: +1 530 400 2774
Email: wes_hardaker@nai.com

Robert Story
Revelstone Software
Phone: +1 770 617 3722
Email: rs-snmp@revelstone.com

Cliff Wang
SmartPipes Inc.
Suite 300, 565 Metro Place South
Dublin, OH 43017
Phone: +1 614 205 0161
E-Mail: cliffwang2000@yahoo.com

7. References

[IPSEC]

Kent, S., and Atkinson, R., "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.

[IKE]

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

[SNMPARCH]

Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks",

[RFC 2571](#), April 1999.

[SMIv1]

Rose, M., and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based Internets", STD 16, [RFC 1155](#), May 1990.

[MIB]

Rose, M., and K. McCloghrie, "Concise MIB Definitions", STD 16, [RFC 1212](#), March 1991.

[TRAPS]

Rose, M., "A Convention for Defining Traps for use with the SNMP", [RFC 1215](#), March 1991.

[SMIv2]

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

[SMITC]

McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, [RFC 2579](#), April 1999.

[SNMPCONF]

McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Conformance Statements for SMIv2", STD 58, [RFC 2580](#), April 1999.

[SNMPv1]

Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", STD 15, [RFC 1157](#), May 1990.

[SNMPv2c]

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

[SNMPv2TM]

Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1906](#), January 1996.

[SNMPv3]

Case, J., Harrington D., Presuhn R., and B. Wijnen,

Internet Draft

IPsec Policy Configuration MIB

June 2002

"Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", [RFC 2572](#), April 1999.

[SNMPUSM]

Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", [RFC 2574](#), April 1999.

[SNMPv2]

Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1905](#), January 1996.

[SNMPAPP]

Levi, D., Meyer, P., and B. Stewart, "SNMPv3 Applications", [RFC 2573](#), April 1999.

[SNMPVACM]

Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", [RFC 2575](#), April 1999.

[SNMPINT]

Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction to Version 3 of the Internet-standard Network Management Framework", [RFC 2570](#), April 1999.

[IPSECPM]

Lortz, V., and Rafalow, L., "IPsec Policy Model White Paper", November 2000.

[IPCP]

Jason, J., Rafalow, L., and Vyncke, E., "IPsec Configuration Policy Model", [draft-ietf-ipsp-config-policy-model-05.txt](#), March 2001.

8. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights

might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances

of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

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

9. Acknowledgments

Many other people contributed thoughts and ideas that influenced this MIB. Some special thanks are in order the following people:

John Gillis	(ADC)		
Jamie Jason	(Intel Corporation)	David Partain	
(Ericsson)			
Lee Rafalow	(IBM)	Jon Saperia	(JDS Consulting)
Eric Vyncke	(Cisco Systems)		

10. Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for

copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

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

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

[Appendix A](#). MIB's Model Conformance:

The following table shows the IPsec Policy MIB's support of the the IPsec Policy Model's conformance objects. It lists the conformance object name and section number, its requirement level (MAY,MUST,etc.), whether the MIB supports it (yes,no,part=partial), and a short indication of where/how the MIB supports it.

Many of the "partially" supported objects are actually "partial" only because the MIB actually allows greater flexibility and reuse by not enforcing relational constraints. These are noted in the table below with a "Sup." field of "part" and a note like "1..1 pol.RuleDef.->pol.Grp.Cont. not forced" (for example), which indicates that the mib does not enforce a strict 1 to 1 mapping and allows a greater number of references within it's tables.

Table of the IPsec Policy MIB's support of the IPsec Policy Model's objects

Sect.		Objects		Req.		Sup.	
		'a..b' indicates cardinality range					
		object names may be abbreviated					

e.g.	IPsec Model Object		
	IPsec MIB Supports With...		
4	"Policy Classes"		
4.1	"Class IPsecPolicyGroup"	MUST	yes
	policyGroupContentsTbl		
4.2	"Class SARule"	MUST	yes

Sect.	Objects	Req.	Sup.
	policyRuleDefinitionTbl::pRuleAction		
4.2.1	"Property PolicyRuleName"	MAY	yes
	policyRuleDefinitionTbl::pRuleName		
4.2.1	"Property Enabled"	MUST	yes
	policyRuleDefinitionTbl::pRuleEnabled		
4.2.1	"Property ConditionListType"	MUST	yes
	conditionTbl::condtionFilterListType		
4.2.1	"Property RuleUsage"	MAY	yes
	policyRuleDefinitionTbl::pruledescription		
4.2.1	"Property Mandatory"	MAY	yes

	always true implicitly		
4.2.1	"Property SequencedActions"	MUST	yes
	always mandatory implicitly		
4.2.1	"Property PolicyRoles"	MAY	NA
	not used in device level model		
4.2.1	"Property PolicyDecisionStrategy"	MAY	yes
	always First Matching implicitly		
4.2.2	"Property ExecutionStrategy"	MUST	yes
	compoundActionsTbl::caExecutionStrategy		
4.2.3	"Property LimitNegotiation"	MAY	yes
	policyRuleDef.Tbl::pRuleLimitNegot.		
4.3	"Class IKERule"	MUST	yes

Sect.	Objects	Req.	Sup.
	ikeActionTbl		
4.3.1	"Property IdentityContexts"	MAY	yes
	ikeRuleId.ContextsTbl::iricId.Context		
4.4	"Class IPsecRuffle"	MUST	yes
	ipsecActionTbl		
4.5	"Assoc. Class IPsecPolicyForEndpoint"	MAY	yes

	policyEndpointToGroupTbl::p.GroupName			
4.5.1	"Reference Antecedent"	MUST	yes	
	0..n policyGroup->policyEndpoints			
4.5.2	"Reference Dependent"	MUST	yes	
	0..1 policyEndpoint->policyGroup			
4.6	"Assoc. Class IPsecPolicyForSystem"	MAY	yes	
	systemPolicyGroupName			
4.6.1	"Reference Antecedent"	MUST	yes	
	0..1 policyGroup->systemPolicyGroupName			
4.6.2	"Reference Dependent"	MUST	yes	
	1..1 systemPolicyGroupName->policyGroup			
4.7	"Aggreg. Class SARuleInPolicyGroup"	MUST	yes	
	policyGrp.Cont.Tbl::pgcGrp.ComponentName			
4.7.1	"Property Priority"	SHOULD	yes	
	policyGroupContentsTbl::pgcPriority			
4.7.2	"Reference GroupComponent"	MUST	part	

Sect.	Objects	Req.	Sup.
	1..1 pol.RuleDef.->pol.Grp.Cont. not forced		
4.7.3	"Reference PartComponent"	MUST	yes
	0..n pol.Grp.Cont.table->pol.RuleDef.Tbl		

4.8	"Aggregation Class SAConditionInRule"	MUST	yes
	policyRuleDefinitionTbl::pRuleName		
4.8.1	"Property GroupNumber"	SHOULD	part
	associated with Octet String, not integer		
4.8.1	"Property ConditionNegated"	SHOULD	yes
	filtersInConditionTbl::ficFilterIsNegated		
4.8.2	"Reference GroupComponent"	MUST	yes
	0..n cond.Tbl->policyRuleDefinitionTbl		
4.8.3	"Reference PartComponent"	MUST	part
	1..n pol.RuleDef.->cond.InRule not forced		
4.9	"Aggreg. Class PolicyActionInSARule"	MUST	yes
	policyRuleDef.Tbl::pRuleAction		
4.9.1	"Reference GroupComponent"	MUST	yes
	0..n actions->policyRuleDefinitionTbl		
4.9.2	"Reference PartComponent"	MUST	yes
	1..n policyRuleDef.Tbl->pRuleAction		
4.9.3	"Property ActionOrder"	SHOULD	yes
	actionsInComp.ActionsEntry::aicaPriority		
5	"Condition and Filter Classes"		

Sect.	Objects	Req.	Sup.
5.1	"Class SACondition"	MUST	yes
	conditionTbl		
5.2	"Class IPHeadersFilter"	SHOULD	yes
	filterTbl::ipfType = addressOrNetwork		
5.3	"Class CredentialFilterEntry"	MAY	yes
	credentialFilterTbl		
5.3.1	"Property MatchFieldName"	MUST	yes
	credentialFilterTbl::crfMatchFieldName		
5.3.2	"Property MatchFieldValue"	MUST	yes
	credentialFilterTbl::crfMatchFieldValue		
5.3.3	"Property CredentialType"	MUST	yes
	credentialFilterTbl::crfCredentialType		
5.4	"Class IPSOFilterEntry"	MAY	yes
	filterTbl::ipfType = classification/authority		
5.4.1	"Property MatchConditionType"	MUST	yes
	filterTbl::ipfType		
5.4.2	"Property MatchConditionValue"	MUST	yes
	filterTbl::ipfClass.Level/ipfAuthority		
5.5	"Class PeerIDPayloadFilterEntry"	MAY	yes
	peerIdentityFilterTbl		
5.5.1	"Property MatchIdentityType"	MUST	yes
	peerIdentityFilterTbl::pifIdentityType		

Sect.	Objects	Req.	Sup.
5.5.2	"Property MatchIdentityValue"	MUST	yes
	peerIdentityFilterTbl::pifIdentityValue		
5.6	"Assoc. Class FilterOfSACondition"	SHOULD	yes
	filtersInCompoundFilterTbl::ficSubfilter		
5.6.1	"Reference Antecedent"	MUST	yes
	1..1 compoundFilter->filter list		
5.6.2	"Reference Dependent"	MUST	yes
	0..n filter Tbls->Compound Filter		
5.7	"Assoc. Class AcceptCredentialFrom"	MAY	yes
	credentialFilterTbl::crfAcceptCredFrom		
5.7.1	"Reference Antecedent"	MUST	yes
	0..n condition->Cred.Mng.Service		
5.7.2	"Reference Dependent"	MUST	yes
	0..n Cred.Mng.Service->condition		
6	"Action Classes"		
6.1	"Class SAAction"	MUST	yes
	policyRuleDefinitionTbl::pRuleAction		
6.1.1	"Property DoActionLogging"	MAY	yes
	actions all have action logging ability		
6.1.2	"Property DoPacketLogging"	MAY	yes
	actions all have packet logging ability		
6.2	"Class SASTaticAction"	MUST	yes

Sect.	Objects	Req.	Sup.
	saStaticActions		
6.2.1	"Property LifetimeSeconds"	MUST	part
	all support, static only with timeFilterTbl.		
6.3	"Class IPsecBypassAction"	SHOULD	yes
	saAcceptAction		
6.4	"Class IPsecDiscardAction"	SHOULD	yes
	saDropAction		
6.5	"Class IKERjectAction"	MAY	yes
	saRejectIKEAction		
6.6	"Class PreconfiguredSAAction"	MUST	yes
	saPreconfiguredActionTbl		
6.6.1	"Property LifetimeKilobytes"	MUST	yes
	saPrecon.ActionTbl::sapActionLifetimeKB		
6.7	"Class PreconfiguredTransportAction"	MUST	yes
	saPrecon.ActionTbl::sapActionType		
6.8	"Class PreconfiguredTunnelAction"	MUST	yes
	saPrecon.ActionTbl::sapActionType		
6.8.1	"Property DFHandling"	MUST	yes

	saPreconfiguredActionTbl::sapDFHandling		
6.9	"Class SANegotiationAction"	MUST	yes
	ikeActionTbl		
6.10	"Class IKENegotiationAction"	MUST	yes

Sect.	Objects	Req.	Sup.
	ikeActionTbl		
6.10.1	"Property MinLifetimeSeconds"	MAY	yes
	saNegot.Param.Tbl::sanMin.LifetimeSeconds		
6.10.2	"Property MinLifetimeKilobytes"	MAY	yes
	saNegot.Param.Tbl::sanMin.LifetimeKB		
6.10.3	"Property IdleDurationSeconds"	MAY	yes
	saNegot.Tbl::sanIdleDurrationSeconds		
6.11	"Class IPsecAction"	MUST	yes
	ipsecActionTbl		
6.11.1	"Property UsePFS"	MUST	yes
	ipsecActionTbl::ipsecUsePFS		
6.11.2	"Property UseIKEGroup"	MAY	yes
	ipsecActionTbl::ipsecUseIkeGroup		
6.11.3	"Property GroupId"	MUST	yes
	ipsecActionTbl::ipsecGroudId		

6.11.4	"Property Granularity"	SHOULD	yes
	ipsecActionTbl::ipsecGranularity		
6.11.5	"Property VendorID"	MAY	yes
	ipsecActionTbl::vendorID		
6.12	"Class IPsecTransportAction"	MUST	yes
	ipsecActionTbl::ipsecMode		
6.13	"Class IPsecTunnelAction"	MUST	yes

Sect.	Objects	Req.	Sup.
	ipsecActionTbl::ipsecMode		
6.13.1	"Property DFHandling"	MUST	yes
	ipsecActionTbl::ipsecDFHandling		
6.14	"Class IKEAction"	MUST	yes
	ikeActionTbl		
6.14.1	"Property ExchangeMode"	MUST	yes
	ikeActionTbl::ikeExchangeMode		
6.14.2	"Property UseIKEIdentityType"	MUST	yes
	ikeIdentityTbl::ikeIdType		
6.14.3	"Property VendorID"	MAY	yes
	ikeActionTbl::ipVendorID		

6.14.4	"Property AggressiveModeGroupId"	MAY	yes
	ikeProposalTbl::ipDhGroup		
6.15	"Class PeerGateway"	MUST	yes
	peerIdentityTbl		
6.15.1	"Property Name"	SHOULD	yes
	peerIdentityTbl::peerIdName		
6.15.2	"Property PeerIdentityType"	MUST	yes
	peerIdentityTbl::peerIdType		
6.15.3	"Property PeerIdentity"	MUST	yes
	peerIdentityTbl::peerIdValue		
6.16	"Assoc. Class PeerGatewayForTunnel"	MUST	yes

Sect.	Objects	Req.	Sup.
	peerIdentityTbl		
6.16.1	"Reference Antecedent"	MUST	yes
	0..n ipsec(tunnel)Actions->peerGateway		
6.16.2	"Reference Dependent"	MUST	yes
	0..n peerGateway->ipsec(tunnel)Action		
6.16.3	"Property SequenceNumber"	SHOULD	yes
	filtersInCompoundFilterTbl::ficPriority		
6.17	"Aggregation Class ContainedProposal"	MUST	yes

	ipsecProposalTbl & ikeActionProposalTbl		
6.17.1	"Reference GroupComponent"	MUST	yes
	0..n proposal->action		
6.17.2	"Reference PartComponent"	MUST	part
	1..n action->proposal not forced.		
6.17.3	"Property SequenceNumber"	MUST	yes
	ispec/ikeAction proposal(s)Priority		
6.18	"Assoc. Class HostedPeerGatewayInformation"	MAY	part
	implicit connection peer gateway->system		
6.18.1	"Reference Antecedent"	MUST	no
6.18.2	"Reference Dependent"	MUST	no
6.19	"Assoc. Class TransformOfPreconfig.Action"	MUST	yes
	saPreconfiguredActionTbl		
6.19.1	"Reference Antecedent"	MUST	yes

Sect.	Objects	Req.	Sup.
	2,4,6 preconfiguredAction-> in/out 1-3		
6.19.2	"Reference Dependent"	MUST	yes
	0..n transform->preconfiguredAction		
6.19.3	"Property SPI"	MUST	yes

	saPrecon.ActionTbl::AH/ESP/IPComp-SPI		
6.19.4	"Property Direction"	MUST	yes
	saPreconfiguredActionTbl::sapSADirection		
6.20	"Assoc. Class PeerGtwy.ForPrecon.Tunnel"	MUST	yes
	saPrecon.ActionTbl::sapPeerGtwy.IdName		
6.20.1	"Reference Antecedent"	MUST	yes
	0..n preconfiguredActon->peerGateway		
6.20.2	"Reference Dependent"	MUST	yes
	0..n peerGateway->precon.Action implicit		
7	"Proposal and Transform Classes"		
7.1	"Abstract Class SAProposal"	MUST	yes
	ipsec/ike/precon./static action objects		
7.1.1	"Property Name"	SHOULD	yes
	ipsec/ike/precon.-ActionProposalName		
7.2	"Class IKEProposal"	MUST	yes
	ikeActionProposalTbl		
7.2.1	"Property CipherAlgo."	MUST	yes
	ikeActionProp.Tbl::ipCipherAlgo.		

Sect.	Objects	Req.	Sup.
7.2.2	"Property HashAlgo."	MUST	yes

	ikeActionProp.Tbl::ipHashAlgo.		
7.2.3	"Property PRFAlgo."	MAY	yes
	ikeActionProp.Tbl::ipPrfAlgo.		
7.2.4	"Property GroupId"	MUST	yes
	ikeActionProp.Tbl::ipDhGroup		
7.2.5	"Property AuthenticationMethod"	MUST	yes
	ikeActionProp.Tbl::ipAuthenticationMethod		
7.2.6	"Property MaxLifetimeSeconds"	MUST	yes
	ikeActionProp.Tbl::ipMaxLifetimeseconds		
7.2.7	"Property MaxLifetimeKilobytes"	MUST	yes
	ikeActionProp.Tbl::ipMaxLifetimeKB		
7.2.8	"Property VendorID"	MAY	yes
	ikeActionProp.Tbl::ipVendorId		
7.3	"Class IPsecProposal"	MUST	yes
	ipsecProposalTbl		
7.4	"Abstract Class SATransform"	MUST	yes
	AH/ESP/IPComp-TransformTbl		
7.4.1	"Property TransformName"	SHOULD	yes
	ipsecProp.Tbl::ipsecProp.TransformName		
7.4.2	"Property VendorID"	MAY	yes
	ext. tables can add vendor transforms		

Sect.	Objects	Req.	Sup.
7.4.3	"Property MaxLifetimeSeconds"	MUST	yes
	saNegot.Param.Tbl::sanMin.LifetimeSeconds		
7.4.4	"Property MaxLifetimeKilobytes"	MUST	yes
	saNegot.Param.Tbl::sanMin.LifetimeKB		
7.5	"Class AHTransform"	MUST	yes
	ahTransformTbl		
7.5.1	"Property AHTransformId"	MUST	yes
	ahTransformTbl::ahtName		
7.5.2	"Property UseReplayPrevention"	MAY	yes
	ahTransformTbl::ahtReplayProtection		
7.5.3	"Property ReplayPreventionWindowSize"	MAY	yes
	ahTransformTbl::ahtReplayWindowSize		
7.6	"Class ESPTransform"	MUST	yes
	espTransformTbl		
7.6.1	"Property IntegrityTransformId"	MUST	yes
	espTransformTbl::esptIntegrityTransformId		
7.6.2	"Property CipherTransformId"	MUST	yes
	espTransformTbl::esptCipherTransformId		
7.6.3	"Property CipherKeyLength"	MAY	yes
	espTransformTbl::esptCipherKeyLength		
7.6.4	"Property CipherKeyRounds"	MAY	yes
	espTransformTbl::esptCipherKeyRounds		

Internet Draft

IPsec Policy Configuration MIB

June 2002

Sect.	Objects	Req.	Sup.
7.6.5	"Property UseReplayPrevention"	MAY	yes
	espTransformTbl::esptReplayPrevention		
7.6.6	"Property ReplayPreventionWindowSize"	MAY	yes
	espTransformTbl::esptReplayWindowSize		
7.7	"Class IPCOMPTransform"	MAY	yes
	ipcompTransformTbl		
7.7.1	"Property Algo."	MUST	yes
	ipcompTransformTbl::ipcompAlgo.		
7.7.2	"Property DictionarySize"	MAY	yes
	ipcompTransformTbl::ipcompDictionarySize		
7.7.3	"Property PrivateAlgo."	MAY	yes
	ipcompTrans.Tbl::ipcompPrivateAlgo.		
7.8	"Assoc. Class SAProposalInSystem"	MAY	part
	implicit, MIB proposals=props. in system.		
7.8.1	"Reference Antecedent"	MUST	yes
	1..1 SAProposal->System		
7.8.2	"Reference Dependent"	MUST	yes
	0..n System->SAProposal		
7.9	"Aggregation Class ContainedTransform"	MUST	yes

	ipsecProp.Tbl::ipsecProp.TransformName		
7.9.1	"Reference GroupComponent"	MUST	yes
	0..n SATransforms->IPsecProposal		

Sect.	Objects	Req.	Sup.
7.9.2	"Reference PartComponent"	MUST	yes
	1..n IPsecProposal->SATransform		
7.9.3	"Property SequenceNumber"	MUST	yes
	ipsecProposalTbl::ipsecProposalsPriority		
7.10	"Assoc. Class SATransformInSystem"	MAY	part
	MIB transforms=transforms in that system		
7.10.1	"Reference Antecedent"	MUST	yes
	1..1 SATransform->SystemInstance		
7.10.2	"Reference Dependent"	MUST	yes
	0..n SystemInstance->SATransform		
8	"IKE Service and Identity Classes"		
8.1	"Class IKEService"	MAY	yes
	implicit		
8.2	"Class PeerIdentityTbl"	MAY	yes
	peerIdentityTbl		

8.2.1	"Property Name"	SHOULD	no	
8.3	"Class PeerIdentityEntry"	MAY	yes	
	peerIdentityTbl::PeerIdentityEntry			
8.3.1	"Property PeerIdentity"	SHOULD	yes	
	peerIdentityTbl::peerIdValue			
8.3.2	"Property PeerIdentityType"	SHOULD	yes	
	peerIdentityTbl::peerIdType			

Sect.	Objects	Req.	Sup.	
8.3.3	"Property PeerAddress"	SHOULD	yes	
	peerIdentityTbl::peerIdAddress			
8.3.4	"Property PeerAddressType"	SHOULD	yes	
	peerIdentityTbl::peerIdAddressType			
8.4	"Class AutostartIKEConfiguration"	MAY	yes	
	autostartIkeTbl			
8.5	"Class AutostartIKESetting"	MAY	yes	
	AutostartIkeEntry			
8.5.1	"Property Phase1Onle"	MAY	part	
	autostarkIke references both phase I/II			
8.5.2	"Property AddressType"	SHOULD	yes	
	autostartIkeTbl::autoIkeAddressType			

8.5.3	"Property SourceAddress"	MUST	yes
	autostartIkeTbl::autoIkeSourceAddress		
8.5.4	"Property SourcePort"	MUST	yes
	autostartIkeTbl::autoIkeSourcePort		
8.5.5	"Property DestinationAddress"	MUST	yes
	autostartIkeTbl::autoIkeDestAddress		
8.5.6	"Property DestinationPort"	MUST	yes
	autostartIkeTbl::autoIkeDestPort		
8.5.7	"Property Protocol"	MUST	yes
	autostartIkeTbl::autoIkeProtocol		

Sect.	Objects	Req.	Sup.
8.6	"Class IKEIdentity"	MAY	yes
	ikeIdentityTbl		
8.6.1	"Property IdentityType"	MUST	yes
	ikeIdentityTbl::ikeIdentityType		
8.6.2	"Property IdentityValue"	MUST	yes
	ikeIdentityTbl::ikeIdentityIdString		
8.6.3	"Property IdentityContexts"	MAY	yes
	ikeIdentityContext		

8.7	"Assoc. Class HostedPeerIdentityTbl"	MAY	part	
+-----+	+-----+	+-----+	+-----+	+-----+
	MIB peerIdTbl=peerIdTbl on that system			
+-----+	+-----+	+-----+	+-----+	+-----+
8.7.1	"Reference Antecedent"	MUST	yes	
+-----+	+-----+	+-----+	+-----+	+-----+
	1..1 peerIdTbl->System			
+-----+	+-----+	+-----+	+-----+	+-----+
8.7.2	"Reference Dependent"	MUST	yes	
+-----+	+-----+	+-----+	+-----+	+-----+
	0..n System->peerIdTbl			
+-----+	+-----+	+-----+	+-----+	+-----+
8.8	"Aggregation Class PeerIdentityMember"	MAY	part	
+-----+	+-----+	+-----+	+-----+	+-----+
	PeerIdentityEntries=peerIdentityTbl rows			
+-----+	+-----+	+-----+	+-----+	+-----+
8.8.1	"Reference Collection"	MUST	yes	
+-----+	+-----+	+-----+	+-----+	+-----+
	1..1 ->PeerIdentityTbl			
+-----+	+-----+	+-----+	+-----+	+-----+
8.8.2	"Reference Member"	MUST	yes	
+-----+	+-----+	+-----+	+-----+	+-----+
	0..n ->PeerIdentityEntry			
+-----+	+-----+	+-----+	+-----+	+-----+
8.9	"Assoc. Class IKEServicePeerGateway"	MAY	yes	
+-----+	+-----+	+-----+	+-----+	+-----+
	ikeActionTbl::ikePeerGatewayName			
+-----+	+-----+	+-----+	+-----+	+-----+

+-----+	+-----+	+-----+	+-----+	+-----+
Sect.	Objects	Req.	Sup.	
+-----+	+-----+	+-----+	+-----+	+-----+
8.9.1	"Reference Antecedent"	MUST	yes	
+-----+	+-----+	+-----+	+-----+	+-----+
	0..n IKEService->PeerGateway			
+-----+	+-----+	+-----+	+-----+	+-----+
8.9.2	"Reference Dependent"	MUST	yes	
+-----+	+-----+	+-----+	+-----+	+-----+
	0..n PeerGateway->IKEService			
+-----+	+-----+	+-----+	+-----+	+-----+
8.10	"Assoc. Class IKEServicePeerIdentityTbl"	MAY	yes	

	peerIdTbl		
8.10.1	"Reference Antecedent"	MUST	yes
	0..n IKEService->peerIDTbl		
8.10.2	"Reference Dependent"	MUST	yes
	0..n peerIDTbl->IKEService		
8.11	"Assoc. Class IKEAutostartSetting"	MAY	part
	implicit, IKEService uses autostartIkeTbl		
8.11.1	"Reference Element"	MUST	yes
	0..n autostarkIkeEntry->IKEService		
8.11.2	"Reference Setting"	MUST	no
	0..n IKEService->autostartIkeEntry		
8.12	"Aggreg. Class AutostartIKESettingContext"	MAY	part
	1< entries in autstartIkeTbl,Comp. Actions		
8.12.1	"Reference Context"	MUST	part
	see above		
8.12.2	"Reference Setting"	MUST	part
	see above		

Sect.	Objects	Req.	Sup.
8.12.3	"Property SequenceNumber"	SHOULD	yes

	autostartIkeTbl::autoIkePriority			
8.13	"Assoc. Class IKEServiceForEndpoint"	MAY	no	
	associates IKEService to Endpoint			
8.13.1	"Reference Antecedent"	MUST	no	
8.13.2	"Reference Dependent"	MUST	no	
8.14	"Assoc. Class IKEAutostartConfiguration"	MAY	part	
	IKEService->autostartIkeTbl on that system			
8.14.1	"Reference Antecedent"	MUST	no	
	0..n IKEService->autostartIKEconifig.			
8.14.2	"Reference Dependent"	MUST	NA	
	0..n autostartIKEConfiguration->IKEService			
8.14.3	"Property Active"	SHOULD	no	
8.15	"Assoc. Class IKEUsesCred.Mng.Service"	MAY	yes	
	CredentialFilterTbl::crfAcctpCredFrom			
8.15.1	"Reference Antecedent"	MUST	yes	
	0..n IKEServie->Cred.Mng.Service			
8.15.2	"Reference Dependent"	MUST	yes	
	0..n Cred.ManagementService->IKEService			
8.16	"Assoc. Class EndpointHasLocalIKEId."	MAY	yes	
	ikeIdentityTbl			
8.16.1	"Reference Antecedent"	MUST	part	

Sect.	Objects	Req.	Sup.
	0..1 IkeIdentity->IPProto.Endpoint not forced		
8.16.2	"Reference Dependent"	MUST	yes
	0..n IPProtocolEndpoint->IkeIdentity		
8.17	"Assoc. Class Collect.HasLocalIKEId."	MAY	part
	1< entries in IKEIdentityTbl, not grouped		
8.17.1	"Reference Antecedent"	MUST	part
	0..1 IkeIdentity->endpointCollection not forced		
8.17.2	"Reference Dependent"	MUST	yes
	0..n endpoints->IkeIdentity		
8.18	"Assoc. Class IKEIdentitiesCredential"	MAY	yes
	associates IKEIdentities to credentials		
8.18.1	"Reference Antecedent"	MUST	yes
	0..n IKEIdentity -> Credentials		
8.18.2	"Reference Dependent"	MUST	yes
	0..n credentials -> IKEIdentity		

