

IPSP Working Group
Internet Draft
[draft-ietf-ipsec-conf-mib-02.txt](#)

M. Baer
Network Associates Inc
R. Charlet
Redcreek Communications
W. Hardaker
Network Associates Inc
D. Partain
Ericsson
J. Saperia
JDS Consulting Inc
C. Wang
Smartpipes Inc
Jul 2001

IPsec Policy Configuration MIB
draft-ietf-ipsec-conf-mib-02.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#). 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 (2001). 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

Various Authors

[Page 2]

Internet Draft

IPsec Policy Configuration MIB

November 2001

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.

Areas where this MIB diverge 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 Lists of conditions and lists of filters within a condition can be defined individually as to whether the subgroupings should be logically ANDed or ORed together. This is different from the IPCP model as that model defines either an ORed set of ANDed filters (Conjunctive Normal Form) or an ANDed set of ORed filters disjunctive normal form (DNF). This MIB is more flexible to make representation and storage easier without dropping functionality.

4. TODO

This MIB is still a work in progress and is changing as the IPCP data model changes. As that model is solidifying, this MIB will also solidify. There are also some known missing features that will be added to future versions of the MIB as development progresses:

- 1) Scheduled policies. (currently policies are always enabled and active)
- 2) Filter types missing. Certain filter types are currently missing from the filter system, like Credential Filters.

Various Authors

[Page 3]

Internet Draft

IPsec Policy Configuration MIB

November 2001

- 3) Notifications. Currently no notifications are defined for policy action failures and report logging.
- 4) Conformance objects. No objects indicating conformance guidelines have currently been defined yet.

Feedback is sought for the work done to date and should be sent to the ipsp working group mailing list (ipsec-policy@vpnc.org).

[5. Definitions](#)

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

IMPORTS

```
    MODULE-IDENTITY, OBJECT-TYPE, Integer32,
    Unsigned32, experimental                FROM SNMPv2-SMI
    TEXTUAL-CONVENTION, RowStatus, TruthValue,
    TimeStamp, StorageType, RowPointer      FROM SNMPv2-TC
-- uncomment when conformance implemented
--    MODULE-COMPLIANCE, OBJECT-GROUP,
--    NOTIFICATION-GROUP                    FROM SNMPv2-CONF
    SnmpAdminString                         FROM SNMP-FRAMEWORK-MIB
    IkeHashAlgorithm, IpsecDoiEncapsulationMode,
    IpsecDoiAhTransform, IpsecDoiIpcompTransform,
    IpsecDoiAuthAlgorithm, IpsecDoiEspTransform,
    IkeGroupDescription, IpsecDoiIdentType,
    IkeEncryptionAlgorithm                  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
Redcreek Communications
3900 Newpark Mall Rd.
Newark, CA 94560
Phone: +1 510 795 6903
Email: rcharlet@redcreek.com

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 5]

Internet Draft

IPsec Policy Configuration MIB

November 2001

Jon Saperia
JDS Consulting, Inc.
174 Chapman Street
Watertown, MA 02472
Phone: +1 617 744 1079
Email: saperia@jdscons.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      "200102230000Z"          -- 23 February 2001
DESCRIPTION   "This is the initial version of this MIB."

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

REVISION      "200111210000Z"          -- 21 November 2001
DESCRIPTION   "Minor updates."
::= { experimental xxx }              -- XXX: change on assignment
```

```
--
-- groups of related objects
--
```

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

```
--
-- Textual Conventions
--
```

```
IpsecBooleanOperator ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "The IpsecBooleanOperator operator is used to specify whether
         sub-components in a decision making process are ANDed or ORed
         together to decide if the resulting expression is true or false."
    SYNTAX      INTEGER { or(0), and(1) }
```

```
IpsecIsNegated ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "The IpsecIsNegated operator is used to specify whether
         or not the results of a sub-components return clause is taken
         as is, or if the logical negation of the result is used instead."
    SYNTAX      INTEGER { yes(0), no(1) }
```

```

--
-- 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.  It's 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 'drop' 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 default action to take when a packet arrives shall be to
        allow the packet to pass through to the next processing point."
    ::= { 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      IpvsecDoiIdentType,
    peEndpointAddress        OCTET STRING,
    peGroupName              SnmpAdminString,
    peLastChanged            TimeStamp,
    peStorageType            StorageType,
    peRowStatus              RowStatus
}

```

```

peEndpointIdentType OBJECT-TYPE
    SYNTAX      IpvsecDoiIdentType { idIpv4Addr(1), idFqdn(2),
                                     idIpv6Addr(5) }
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The IpvsecDoiIdentType defining the address format associated with a
        given endpoint.  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.  It is
        implementation dependent as to which values of the
        IpvsecDoiIdentType are supported.  However, devices supporting
        IPv4 MUST support the idIpv4Addr value, and devices
        supporting IPv6 MUST support the idIpv6Addr value."
    ::= { policyEndpointToGroupEntry 1 }

```

```

peEndpointAddress OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..64))
    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 the group referenced by the peGroupName object exists within the policyGroupContentsTable."

::= { 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,

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

Various Authors

[Page 10]

Internet Draft IPsec Policy Configuration MIB November 2001

DESCRIPTION
"The priority (sequence number) of the sub-component in this group."
 ::= { policyGroupContentsEntry 2 }

pgcGroupComponentType OBJECT-TYPE
SYNTAX INTEGER { reserved(0), group(1), policy(2) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"Indicates whether the pgcGroupComponentName object is the name of another group contained within this table or whether it is the of name a policy and should be looked up in the policyRuleDefinitionTable table."
 ::= { policyGroupContentsEntry 3 }

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 4 }

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 5 }

```
pgcStorageType 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 }
    ::= { policyGroupContentsEntry 6 }
```

```
pgcRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
```

Various Authors

[Page 11]

Internet Draft

IPsec Policy Configuration MIB

November 2001

```
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 7 }
```

```
--
-- 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 set of
    filtering conditions to an action to be executed when the
    filtering conditions have been met."
```

```
::= { ipsecPolicyConfigObjects 4 }
```

```
policyRuleDefinitionEntry OBJECT-TYPE
```

```
SYNTAX      PolicyRuleDefinitionEntry
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
"A row defining a particular policy definition. The pRuleName object is used to match a set of conditionsInRuleEntries which defines the set of conditions associated with this rule."
```

```
INDEX      { pRuleName, pRuleType }
```

```
::= { policyRuleDefinitionTable 1 }
```

```
PolicyRuleDefinitionEntry ::= SEQUENCE {
```

```
  pRuleName          SnmpAdminString,
```

```
  pRuleType          INTEGER,
```

```
  pRuleDescription   OCTET STRING,
```

```
  pRuleConditionListType IpsecBooleanOperator,
```

```
  pRuleAction        RowPointer,
```

```
  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 }
```

```
pRuleType OBJECT-TYPE
```

```
SYNTAX      INTEGER { reserved(0), ipsec(1), ike(2) }
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
"The policy rule type. See [XXX:  
draft-ietf-ipsp-config-policy-model-04.txt section 4 for when
```

```
to process which rule type]."  
 ::= { policyRuleDefinitionEntry 2 }
```

```
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 { 'H' }  
 ::= { policyRuleDefinitionEntry 3 }
```

```
pRuleConditionListType OBJECT-TYPE  
SYNTAX      IsecBooleanOperator  
MAX-ACCESS  read-create  
STATUS      current  
DESCRIPTION  
    "pRuleConditionListType specifies whether the list of associated  
    conditions within this rule is an ANDed list or an ORed list."  
DEFVAL { and }  
 ::= { policyRuleDefinitionEntry 4 }
```

```
pRuleAction OBJECT-TYPE  
SYNTAX      RowPointer  
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  
saStaticActionTable  
saPreconfiguredActionTable  
ikeActionTable  
ipsecActionTable
```

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 }
```

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 6 }
```

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 7 }
```

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 8 }

--
-- ikeRuleIdentityContextsTable
--

ikeRuleIdentityContextsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IkeRuleIdentityContextsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Contains a list of contexts associated with a given IKE rule.
         Multiple entries in this table for a given pRuleName are
         considered to be logically ORed together."
    ::= { ipsecPolicyConfigObjects 5 }

ikeRuleIdentityContextsEntry OBJECT-TYPE
    SYNTAX      IkeRuleIdentityContextsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row defining an entry in a given context list."
    INDEX      { pRuleName, iricIndex }
    ::= { ikeRuleIdentityContextsTable 1 }

IkeRuleIdentityContextsEntry ::= SEQUENCE {
    iricIndex          Integer32,
    iricIdentityContext OCTET STRING,
    iricLastChanged   TimeStamp,
    iricStorageType   StorageType,
    iricRowStatus     RowStatus
}

iricIndex OBJECT-TYPE
    SYNTAX      Integer32 (0..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A numeric index number of a given context."
    ::= { ikeRuleIdentityContextsEntry 1 }

iricIdentityContext OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..511))

```

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"pgIKEidentityContexts is a string that corresponds to an ANDed list of values. This property is used to establish a phase 1 IKE SA by using this property in conjunction with the UseIKEIdentityType property in the corresponding IKEAction. These two properties are then used to find an appropriate IKEIdentity object for use on the protected IPProtocolEndpoint."

::= { ikeRuleIdentityContextsEntry 2 }

iricLastChanged 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."

::= { ikeRuleIdentityContextsEntry 3 }

iricStorageType 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 }

::= { ikeRuleIdentityContextsEntry 4 }

iricRowStatus 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 can not be set to active unless a corresponding row in the policyRuleDefinitionsTable exists and is marked as an ike rule."

```
::= { ikeRuleIdentityContextsEntry 5 }
```

```
--
```

```
-- Policy conditions in a rule table
```

```
--
```

```
conditionsInRuleTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF ConditionsInRuleEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"The list of conditions associated with a policy rule.  
In particular, an pRuleName can be used to get a list of  
corresponding conditionName's, which can then be used to look  
up a given condition's parameters by referring to the  
conditionTable."
```

```
::= { ipsecPolicyConfigObjects 6 }
```

```
conditionsInRuleEntry OBJECT-TYPE
```

```
SYNTAX ConditionsInRuleEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"conditionsInRuleEntry specifies a given condition as  
associated with a given rule."
```

```
INDEX { pRuleName, conditionSequenceNumber }
```

```
::= { conditionsInRuleTable 1 }
```

```
ConditionsInRuleEntry ::= SEQUENCE {
```

```
conditionSequenceNumber Integer32,  
conditionIsNegated IpsecIsNegated,  
conditionName SnmpAdminString,  
conditionRuleLastChanged TimeStamp,  
conditionRuleStorageType StorageType,  
conditionRuleRowStatus RowStatus
```

```
}
```

```
conditionSequenceNumber OBJECT-TYPE
```

```
SYNTAX Integer32 (1..65536)
```

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

```
STATUS current
```

```
DESCRIPTION
```

"conditionSequenceNumber is the priority of the conditionName in this row. This represents the order that conditions should be processed in a Rule. Lower values are processed first."
 ::= { conditionsInRuleEntry 2 }

conditionIsNegated OBJECT-TYPE
SYNTAX IpsecIsNegated
MAX-ACCESS read-create

Various Authors

[Page 17]

Internet Draft

IPsec Policy Configuration MIB

November 2001

STATUS current
DESCRIPTION
"conditionIsNegated indicates whether the condition results should be negated (e.g. if a boolean 'not' is performed on the condition)."
DEFVAL { no }
 ::= { conditionsInRuleEntry 3 }

conditionName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"conditionName is the name of the condition associated with the conditionRuleName."
 ::= { conditionsInRuleEntry 4 }

conditionRuleLastChanged 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."
 ::= { conditionsInRuleEntry 5 }

conditionRuleStorageType 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 }
::= { conditionsInRuleEntry 6 }

conditionRuleRowStatus 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.

For a row in the conditionInRuleTable to change to the active state, the row in the conditionTable that is indicated by conditionName must be active and the row in the XXX: rowTable/saRowTable? indicated by conditionRuleName must be active. No conditions are necessary to become inactive, although the rows in conditionTable and XXX: rowTable/saRowTable? should be active at all times that this row is active. "

::= { conditionsInRuleEntry 7 }

--
-- compound actions table
--

compoundActionsTable OBJECT-TYPE

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

""

::= { ipsecPolicyConfigObjects 7 }

compoundActionsEntry OBJECT-TYPE

SYNTAX CompoundActionsEntry
MAX-ACCESS not-accessible
STATUS current

DESCRIPTION

""

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."

::= { 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."

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 8 }

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   RowPointer,

```

```

    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 RowPointer

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

compoundActionsTable - Allowing recursion
saPreconfiguredActionTable
ikeActionTable
ipsecActionTable

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.

XXX: and if the row above disappears from underneath it? Should we define a notification?"

::= { 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 }

--

-- Policy condition definitions table

--

conditionTable OBJECT-TYPE

SYNTAX SEQUENCE OF ConditionEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A table of conditions and their associated parameters."

::= { ipsecPolicyConfigObjects 9 }

conditionEntry OBJECT-TYPE

SYNTAX ConditionEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An entry in the conditions table. A condition listed in this table is considered to have a successful return value if and only if all of the filters associated with the condition, as defined in the filtersInConditionTable, are all true

themselves (after applying any negation as defined by the `ficFilterIsNegated` object). IE, filter results are always ANDed together.

XXX: the only functional data in this table is the `conditionUsage` object. Should this get moved into the `conditionsInRuleTable` instead (which changes the semantics of how things work)? It really does belong here though, but moving it up would reduce the table count."

```
INDEX          { conditionName }
 ::= { conditionTable 1 }
```

```
ConditionEntry ::= SEQUENCE {
    conditionDescription          OCTET STRING,
    conditionUsage                BITS,
    conditionFilterListType      IpsecBooleanOperator,
    conditionLastChanged         TimeStamp,
    conditionStorageType         StorageType,
    conditionRowStatus           RowStatus
}
```

```
conditionDescription 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' }
    ::= { conditionEntry 1 }
```

```
conditionUsage OBJECT-TYPE
    SYNTAX          BITS { onBoot(0),
                          onManual(1),
                          onDataTraffic(2),
                          onIKEMessage(3)
                        }
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "Defines when this condition is to be used."
```

If the condition type includes:

onBoot:

The condition is considered to be true at the boot time of the ipsec policy system and the rules are initially

checked for this condition. Filters defined in the filtersInCondition table are ignored for purposes of evaluating the condition results in this case.

onManual:

The condition is considered to be true when the ipsec policy system is processing the rule(s) as a result of an appropriate administrative operation, such as the pushing of a XXX:insert-object-from-non-existent-button-table button. Filters defined in the filtersInCondition table are ignored for purposes of evaluating the condition results in this case.

onDataTraffic:

This condition is considered to be true when evaluated when traffic is processed by it and all filters results defined by the filtersInConditionsTable are also evaluated to be true (I.E., the filter results are ANDed together).

onIKEMessage:

This condition is considered to be true when evaluated when IKE related traffic is processed by it and all filters results defined by the filtersInConditionsTable are also evaluated to be true (I.E., the filter results are ANDed together)."

::= { conditionEntry 2 }

conditionFilterListType 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 }

```
::= { conditionEntry 3 }
```

conditionLastChanged 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."

```
::= { conditionEntry 4 }
```

conditionStorageType OBJECT-TYPE

SYNTAX StorageType

Various Authors

[Page 25]

Internet Draft

IPsec Policy Configuration MIB

November 2001

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 }

```
::= { conditionEntry 5 }
```

conditionRowStatus 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 can not be made active until the conditionUsage object has been defined. Until that point the object should return a notReady state when queried and any attempts to set it to active will result in a inconsistentValue error.

Once active, it may not have its value changed if any active rows in the conditionsInRuleTable have a conditionName

matching the conditionName of this row.

XXX: must at least one filter be defined? Only if type above is related to traffic? Should we create a 'true' filter type to allow an explicit forced always true condition to be created?"
 ::= { conditionEntry 6 }

--
-- Policy filters in a condition table
--

filtersInConditionTable OBJECT-TYPE
SYNTAX SEQUENCE OF FiltersInConditionEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"This table defines a list of filters contained within a given condition defined in the conditionTable."
 ::= { ipsecPolicyConfigObjects 10 }

Various Authors

[Page 26]

Internet Draft IPsec Policy Configuration MIB November 2001

filtersInConditionEntry OBJECT-TYPE
SYNTAX FiltersInConditionEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"An entry into the list of filters for a given condition. An entry row here maps a conditionName to a filterName which can be used as an index into the filterTable to retrieve the filter's definition."
INDEX { conditionName, filterName }
 ::= { filtersInConditionTable 1 }

FiltersInConditionEntry ::= SEQUENCE {
ficOnDestination BITS,
ficFilterIsNegated IpsecIsNegated,
ficLastChanged TimeStamp,
ficStorageType StorageType,
ficRowStatus RowStatus
}

ficOnDestination OBJECT-TYPE

SYNTAX INTEGER { reserved(0), source(1), destination(2),
mirrored(3) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Whether the filter is to be applied to the source or the destination address. 'mirrored' means that the filter must match both the source and the destination components of the packet to evaluate to true. Note that certain types of filters will ignore this object's value when filtering on packet contents that are not tied to a direction (E.G. protocol type)."

::= { filtersInConditionEntry 1 }

ficFilterIsNegated OBJECT-TYPE

SYNTAX IpsecIsNegated

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Indicates whether the result of applying this filter should be negated or not. If the ficOnDestination object is set to both source and destination, the negation is applied after the source and destination results are returned and ANDed together. IE, result = !(filter(source) && filter(destination))."

DEFVAL { no }

::= { filtersInConditionEntry 2 }

ficLastChanged 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."

::= { filtersInConditionEntry 3 }

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 }  
 ::= { filtersInConditionEntry 4 }
```

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 filterName object is both defined and it's row is active in the filterTable. An attempt to do so will result in an inconsistentValue error.

XXX: indicate minimum conditions allowed when transitioning between non-active and active states (both directions). IE, which sub/super-table rows must be of the requested stated? Which columns must be defined for this row to be operational?"

```
 ::= { filtersInConditionEntry 5 }
```

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

filterTable OBJECT-TYPE

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

"This table contains a list of filter definitions to be used within the filtersInConditionTable."

```
 ::= { ipsecPolicyConfigObjects 11 }
```



```

filterEntry OBJECT-TYPE
    SYNTAX      FilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A definition of a particular filter."
    INDEX       { filterName }
    ::= { filterTable 1 }

```

```

FilterEntry ::= SEQUENCE {
    filterName                SnmpAdminString,
    filterType                INTEGER,
    filterExternalOID         RowPointer,
    filterAddressType         IpsecDoiIdentType,
    filterAddress             OCTET STRING,
    filterProtocol            Integer32,
    filterLowPort             Integer32,
    filterHighPort           Integer32,
    filterClassificationLevel Integer32,
    filterAuthority           Integer32,
    filterLastChanged         TimeStamp,
    filterStorageType         StorageType,
    filterRowStatus           RowStatus
}

```

```

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

```

```

filterType OBJECT-TYPE
    SYNTAX      INTEGER { reserved(0), external(1),
                        addressOrNetwork(2),
                        protocol(3), portRange(4), credential(5),
                        classification(6), authority(7) }
    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 instance 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:

external:

- XXX: To be defined later.

addressOrNetwork:

- Tests for address or network matches using the filterAddressType and filterAddress objects to specify match conditions for the data packet being processed.

A row in this table of the type addressOrNetwork will cause the filterRowStatus object to return the notReady state if the filterAddressType object or the filterAddress object have not been appropriately configured.

protocol:

- Tests to see if the packet being processed matches against the given protocol type.

A row in this table of the type addressOrNetwork will cause the filterRowStatus object to return the notReady state if the filterProtocol object has not been appropriately configured.

portRange:

- Tests to see if the portnumber used by the protocol falls within a starting and ending pair of port numbers, which is defined by the the filterLowPort and filterHighPort objects. To filter on an exact port, the filterLowPort and filterHighPort objects should be set to the same value.

A row in this table of the type portRange will cause the filterRowStatus object to return the notReady state if the filterLowPort or filterHighPort objects have not been

Internet Draft

IPsec Policy Configuration MIB

November 2001

appropriately configured.

credential:

- Tests to see if the incoming packet matches against the credentials of the IKE peer.

XXX: todo

classification:

- Tests to see if the classification level of the incoming packet matches the classification level specified by the filterClassificationLevel object. If it does not match, or if the incoming packet does not have a classification level associated with it, this filter is considered to have a unsuccessful return status.

A row in this table of the type classification will cause the filterRowStatus object to return the notReady state if the filterClassificationLevel object has not been appropriately configured.

authority:

- Tests to see if the protection authority source of the incoming packet matches the authority source specified by the filterAuthority object. If it does not match, or if the incoming packet does not have a protection authority associated with it, this filter is considered to have a unsuccessful return status.

A row in this table of the type authority will cause the filterRowStatus object to return the notReady state if the filterAuthority object has not been appropriately configured.

"

```
::= { filterEntry 2 }
```

filterExternalOID OBJECT-TYPE

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

```
    "XXX: To be defined later."
```

```
::= { filterEntry 3 }
```

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

DESCRIPTION

"The transport domain that will be used to help define the semantics of the addressOrNetwork, addressRange, and protocol tests.

For addressOrNetwork and addressRange tests, if the filterDomain address type does match the address type to be tested against, the filter result is to be considered a failure.

For the portRange test, if the filterDomain does not specify a port number, the filter result is considered to be a failure.

For protocol tests, if the filterDomain object's protocol specification does not match the protocol of the packet the filter is being applied to, the filter result is to be considered a failure."

::= { filterEntry 4 }

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

DESCRIPTION

"The address to use when performing an addressOrNetwork test.

For an addressOrNetwork test, the filterAddress and filterMask pair define an address or set of addresses to match the address from the incoming packet against. The filterMask defines which bits of the filterAddress and incoming address the test should be performed against. Any differing bits in the masked portion of the two addresses indicates a test failure.

If a port number is required by the corresponding TDomain

defined in the filterDomain object, it can be given any value in this object as it will not be used in the test."
 ::= { filterEntry 5 }

filterProtocol OBJECT-TYPE

SYNTAX Integer32 (0..64)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { filterEntry 6 }

filterLowPort OBJECT-TYPE

SYNTAX Integer32 (0..65536)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { filterEntry 7 }

filterHighPort OBJECT-TYPE

SYNTAX Integer32 (0..65536)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { filterEntry 8 }

filterClassificationLevel OBJECT-TYPE

SYNTAX INTEGER { topSecret(61),
secret(90),
confidential(150),
unclassified(171) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The classification level at which the classification test

must match against for the filter to be considered successful."
 ::= { filterEntry 9 }

filterAuthority OBJECT-TYPE

SYNTAX INTEGER { genser(0), stopEsi(1), sci(2), nsa(3), doe(4) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The authority for which the authority test must match against
 for the filter to be considered successful."

::= { filterEntry 10 }

filterLastChanged 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."

::= { filterEntry 11 }

filterStorageType 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 }

::= { filterEntry 12 }

filterRowStatus 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 filterType 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 filterType object description for further details."

```
::= { filterEntry 13 }
```

```
--
```

```
-- Static Action Table
```

```
--
```

```
saStaticActionTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF SaStaticActionEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"This table lists a list of non-negotiated IPsec actions that can be performed."
```

```
::= { ipsecPolicyConfigObjects 12 }
```

```
saStaticActionEntry OBJECT-TYPE
```

```
SYNTAX SaStaticActionEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"One entry in the saStaticActionTable."
```

```
INDEX { sasActionName }
```

```
::= { saStaticActionTable 1 }
```

```
SaStaticActionEntry ::= SEQUENCE {
```

```
  sasActionName          SnmpAdminString,  
  sasActionDescription   OCTET STRING,  
  sasActionType          INTEGER,  
  sasActionLifetimeSec   Unsigned32,  
  sasActionLifetimeKB    Unsigned32,  
  sasDoActionLogging     TruthValue,  
  sasDoPacketLogging     TruthValue,  
  sasLastChanged         TimeStamp,  
  sasStorageType        StorageType,
```

```
    sasRowStatus                               RowStatus
}
```

```
sasActionName OBJECT-TYPE
  SYNTAX      SnmpAdminString (SIZE(1..32))
  MAX-ACCESS  not-accessible
  STATUS      current
  DESCRIPTION
    "This object contains the name of this SaStaticActionEntry. This row
    can be referred to by an actionsInRuleEntry."
  ::= { saStaticActionEntry 1 }
```

```
sasActionDescription 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 in human terms what the action does"
  DEFVAL { 'H' }
  ::= { saStaticActionEntry 2 }
```

```
sasActionType OBJECT-TYPE
  SYNTAX      INTEGER { bypass(0), discard(1), rejectIke(2) }
  MAX-ACCESS  read-create
  STATUS      current
  DESCRIPTION
    "This object specifies the action taken on the packet.
    0 - bypass the packet
    1 - drop the packet
    2 - reject IKE negotiation."
  ::= { saStaticActionEntry 3 }
```

```
sasActionLifetimeSec OBJECT-TYPE
  SYNTAX      Unsigned32
  MAX-ACCESS  read-create
  STATUS      current
  DESCRIPTION
    "sasActionLifetimeSec specifies how long, in seconds, the
    security association derived from this action should be used."
  ::= { saStaticActionEntry 4 }
```


sasActionLifetimeKB OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"sasActionLifetimeKB specifies how long, in kilobytes the security association derived from this action should be used."
 ::= { saStaticActionEntry 5 }

sasDoActionLogging OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"sasDoActionLogging specifies whether or not an audit message should be logged when the action is performed."
 ::= { saStaticActionEntry 6 }

sasDoPacketLogging OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"sasDoLogging specifies whether or not an audit message should be logged when a packet is processed."
 ::= { saStaticActionEntry 7 }

sasLastChanged 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."
 ::= { saStaticActionEntry 8 }

sasStorageType OBJECT-TYPE
SYNTAX StorageType
MAX-ACCESS read-create

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 }

::= { saStaticActionEntry 9 }

sasRowStatus 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.

XXX: indicate minimum conditions allowed when transitioning between non-active and active states (both directions). IE, which sub/super-table rows must be of the requested stated? Which columns must be defined for this row to be operational?"

::= { saStaticActionEntry 10 }

--

-- Preconfigured Action Table

--

saPreconfiguredActionTable OBJECT-TYPE

SYNTAX SEQUENCE OF SaPreconfiguredActionEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This table lists a list of non-negotiated IPsec actions that can be performed."

::= { ipsecPolicyConfigObjects 13 }

saPreconfiguredActionEntry OBJECT-TYPE

SYNTAX SaPreconfiguredActionEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"One entry in the saPreconfiguredActionTable."

INDEX { sapActionName }

```
 ::= { saPreconfiguredActionTable 1 }
```

```
SaPreconfiguredActionEntry ::= SEQUENCE {
    sapActionName                SnmpAdminString,
    sapActionDescription          OCTET STRING,
    sapActionLifetimeSec         Unsigned32,
    sapActionLifetimeKB         Unsigned32,
    sapDoActionLogging           TruthValue,
    sapDoPacketLogging           TruthValue,
    sapDFHandling                INTEGER,
    sapActionType                IpsecDoiEncapsulationMode,
    sapAHSPI                     Integer32,
    sapAHTransformName           SnmpAdminString,
    sapAHSharedSecretName       SnmpAdminString,
    sapESPSPI                    Integer32,
    sapESPTransformName         SnmpAdminString,
    sapESPEncSharedSecretName   SnmpAdminString,
    sapESPAuthSharedSecretName SnmpAdminString,
    sapIPCompSPI                Integer32,
    sapIPCompTransformName      SnmpAdminString,
    sapPeerGatewayAddressType   IpsecDoiIdentType,
    sapPeerGatewayAddress       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. This row can be referred to by an
     actionsInRuleEntry."
```

```
 ::= { saPreconfiguredActionEntry 1 }
```

```
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 in human terms what the action does"
```

```
 ::= { saPreconfiguredActionEntry 2 }
```

sapActionLifetimeSec OBJECT-TYPE
SYNTAX Unsigned32

Various Authors

[Page 38]

Internet Draft

IPsec Policy Configuration MIB

November 2001

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { saPreconfiguredActionEntry 3 }

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."

::= { saPreconfiguredActionEntry 4 }

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."

::= { saPreconfiguredActionEntry 5 }

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."

::= { saPreconfiguredActionEntry 6 }

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."
 ::= { saPreconfiguredActionEntry 7 }

```

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."

```

```

 ::= { saPreconfiguredActionEntry 8 }

```

sapAHSPI OBJECT-TYPE

```

SYNTAX      Integer32
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION

```

```

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

```

```

 ::= { saPreconfiguredActionEntry 9 }

```

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 10 }

```

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 sharedSecretsTable which holds the pertinent keying
information for the AH SA."
 ::= { saPreconfiguredActionEntry 11 }

sapESPSPi OBJECT-TYPE

SYNTAX Integer32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object represents the SPI value for the ESP SA."
 ::= { saPreconfiguredActionEntry 12 }

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 13 }

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 sharedSecretsTable which holds the pertinent keying
information for the encryption algorithm of the ESP SA."
 ::= { saPreconfiguredActionEntry 14 }

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 sharedSecretsTable which holds the pertinent keying information for the authentication algorithm of the ESP SA."
 ::= { saPreconfiguredActionEntry 15 }

sapIPCompSPI OBJECT-TYPE

SYNTAX Integer32
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object represents the SPI value for the IPComp SA."
 ::= { saPreconfiguredActionEntry 16 }

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 17 }

sapPeerGatewayAddressType OBJECT-TYPE

SYNTAX IsecDoiIdentType
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the address type of the address of the peer for tunnel SAs. This object is used when initiating a tunnel SA. This object is not used for transport SAs. The only valid values for this object are single addresses, not ranges or subnets."
 ::= { saPreconfiguredActionEntry 18 }

sapPeerGatewayAddress OBJECT-TYPE

SYNTAX OCTET STRING
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the address of the peer gateway in a

tunnel SA. This object is used when initiating a tunnel SA. This object is not used for transport SAs."
 ::= { 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.

XXX: indicate minimum conditions allowed when transitioning between non-active and active states (both directions). IE, which sub/super-table rows must be of the requested stated? Which columns must be defined for this row to be operational?"

::= { 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 14 }

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

Various Authors

[Page 45]

Internet Draft

IPsec Policy Configuration MIB

November 2001

"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

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 15 }

ikeActionEntry OBJECT-TYPE

SYNTAX IkeActionEntry

MAX-ACCESS not-accessible

```
STATUS          current
DESCRIPTION
    "The ipsecActionEntry lists the IKE negotiation attributes."
INDEX          { ikeActionName }
::= { ikeActionTable 1 }
```

```
IkeActionEntry ::= SEQUENCE {
    ikeActionName          SnmpAdminString,
```

Various Authors

[Page 46]

Internet Draft

IPsec Policy Configuration MIB

November 2001

```
    ikeActionParametersName          SnmpAdminString,
    ikeThresholdDerivedKeys          Integer32,
    ikeExchangeMode                  INTEGER,
    ikeAgressiveModeGroupId          IkeGroupDescription,
    ikeIdentityName                  SnmpAdminString,
    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."
 ::= { 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."
 ::= { ikeActionEntry 4 }

ikeAggressiveModeGroupId OBJECT-TYPE

Various Authors

[Page 47]

Internet Draft

IPsec Policy Configuration MIB

November 2001

SYNTAX IkeGroupDescription
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The values to be used for Diffie-Hellman exchange."
 ::= { ikeActionEntry 5 }

ikeIdentityName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This row refers to an ikeIdentityEntry in the ikeIdentityTable."
 ::= { ikeActionEntry 6 }

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 7 }

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 8 }

ikeActionRowStatus OBJECT-TYPE
SYNTAX RowStatus
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."
 ::= { ikeActionEntry 9 }

--
-- 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 16 }

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 17 }
```

```
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     INTEGER,
    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      INTEGER { desCbc(1), ideaCbc(2), blowfishCbc(3),
                    rc5Rc16B64Cbc(4), tripleDesCbc(5), castCbc(6) }
MAX-ACCESS  read-create
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 mib 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 mib 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 pseudo-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
DESCRIPTION

"The VendorID property is used to identify vendor-defined key exchange GroupIDs."
 ::= { ikeProposalEntry 7 }

ipDhGroup OBJECT-TYPE

Internet Draft

IPsec Policy Configuration MIB

November 2001

```
SYNTAX      IkeGroupDescription
```

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

```
STATUS      current
```

```
DESCRIPTION
```

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

```
::= { ikeProposalEntry 8 }
```

```
ipAuthenticationMethod OBJECT-TYPE
```

```
SYNTAX      INTEGER { digitalSignature(1), pubKeyEncryption(2),
                      revisedPubKeyEncryption(3), preSharedKey(4) }
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "This mib 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

Various Authors

[Page 53]

Internet Draft

IPsec Policy Configuration MIB

November 2001

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 18 }

```

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

```

```

IsecActionEntry ::= SEQUENCE {
    ipsecActionName          SnmpAdminString,
    ipsecActionParametersName SnmpAdminString,
    ipsecUsePfs              TruthValue,
}

```

```

    ipsecVendorId          OCTET STRING,
    ipsecGroupId           IkeGroupDescription,
    ipsecUseIkeGroup       TruthValue,
    ipsecGranularity       INTEGER,
    ipsecMode              INTEGER,
    ipsecDFHandling        INTEGER,
    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  not-accessible
    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 }
```

```
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 3 }
```

```
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 4 }
```

```
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 5 }
```

```
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 ignore."
```

```
::= { ipsecActionEntry 6 }
```

ipsecGranularity OBJECT-TYPE
SYNTAX INTEGER { wideSelector(1), narrowSelector(2)}
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object specifies the how the proposed selector for the security association will be created.
For wideSelector (1) choice, the selector is created by using the FilterList information. The selector can be subnet or range address.
For narrowSelector(2), the selector is created by using the traffic parameters (i.e., the 5-tuple of the traffic). "
 ::= { ipsecActionEntry 7 }

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."
 ::= { ipsecActionEntry 8 }

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 9 }

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 10 }

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 11 }

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.

XXX: indicate minimum conditions allowed when transitioning between non-active and active states (both directions). IE, which sub/super-table rows must be of the requested stated? Which columns must be defined for this row to be operational?"

::= { ipsecActionEntry 12 }

--

-- ipsecProposalsInActionTable

--

ipsecProposalTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpsecProposalEntry

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 19 }

ipsecProposalEntry OBJECT-TYPE
SYNTAX      IpsecProposalEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "An entry containing the information on an IPsec proposal."
INDEX       { ipsecActionName, ipsecProposalName, ipsecProposalType,
              ipsecProposalPriority }
 ::= { ipsecProposalTable 1 }

IpsecProposalEntry ::= SEQUENCE {
    ipsecProposalName          SnmpAdminString,
    ipsecProposalType          INTEGER,
    ipsecProposalPriority      Integer32,
    ipsecProposalTransformName SnmpAdminString,
    ipsecProposalLastChanged   TimeStamp,
    ipsecProposalStorageType   StorageType,
    ipsecProposalRowStatus     RowStatus
}

ipsecProposalName OBJECT-TYPE
SYNTAX      SnmpAdminString (SIZE(1..32))
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "The proposal name contained within a given ipsecAction"
 ::= { ipsecProposalEntry 1 }

ipsecProposalType OBJECT-TYPE
SYNTAX      INTEGER { reserved(0), esp(1), ah(2), ipcomp(3) }
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION

```

"An ipsecProposal informs a system which protocol or combination of protocols to build an SA (bundle) with. Only a certian few combinations are sensible."
 ::= { ipsecProposalEntry 2 }

ipsecProposalPriority OBJECT-TYPE

SYNTAX Integer32 (0..65535)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The priority level (AKA sequence level) of given proposal transform within a proposal set of ipsecProposalType. 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."

::= { ipsecProposalEntry 3 }

ipsecProposalTransformName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The name for the given transform which can be used to lookup the transform's specific parameters in the ahTransformTable, the espTransformTable or the ipcompTransformTable."

::= { ipsecProposalEntry 4 }

ipsecProposalLastChanged 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."

::= { ipsecProposalEntry 5 }

ipsecProposalStorageType 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."

::= { ipsecProposalEntry 6 }

Internet Draft

IPsec Policy Configuration MIB

November 2001

ipsecProposalRowStatus 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.

XXX: indicate minimum conditions allowed when transitioning between non-active and active states (both directions). IE, which sub/super-table rows must be of the requested stated? Which columns must be defined for this row to be operational?"

::= { ipsecProposalEntry 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 20 }

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,

```

Various Authors

[Page 60]

Internet Draft

IPsec Policy Configuration MIB

November 2001

```

    ahtAlgorithm           IpvsecDoiAhTransform,
    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 ipsecProposalEntry."

::= { 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.

XXX: indicate minimum conditions allowed when transitioning

between non-active and active states (both directions). IE, which sub/super-table rows must be of the requested stated? Which columns must be defined for this row to be operational?"

::= { 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 21 }

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,
    esptIntegrityTransformId IpsecDoiAuthAlgorithm,
    esptReplayPrevention TruthValue,
    esptReplayWindowSize Unsigned32,
    esptLastChanged TimeStamp,
    esptStorageType StorageType,
    esptRowStatus RowStatus
}
```

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

```
DESCRIPTION
    "The name of this particular espTransform be referred to by an
    ipsecProposalEntry."
 ::= { 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 IsecDoiEspTransform
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This mib 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 mib 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
DESCRIPTION
"This mib object specifies the number of key rounds for

the ESP cipher algorithm."
 ::= { espTransformEntry 6 }

esptIntegrityTransformId OBJECT-TYPE
SYNTAX IsecDoiAuthAlgorithm
MAX-ACCESS read-create
STATUS current
DESCRIPTION

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

esptReplayPrevention OBJECT-TYPE

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

DESCRIPTION

```
    "esptReplayPrevention indicates wether 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
    created through an external process may have a storage type of
```

```

        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.

        XXX: indicate minimum conditions allowed when transitioning
        between non-active and active states (both directions).  IE,
        which sub/super-table rows must be of the requested stated?
        Which columns must be defined for this row to be operational?"
 ::= { 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 22 }

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 particular ipcompTransformEntry. This row will be referred to by an ipsecProposalEntry."

::= { 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 IpsecDoiIpcompTransform

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 feild 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

Various Authors

[Page 68]

Internet Draft

IPsec Policy Configuration MIB

November 2001

"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.

XXX: indicate minimum conditions allowed when transitioning between non-active and active states (both directions). IE, which sub/super-table rows must be of the requested stated? Which columns must be defined for this row to be operational?"

::= { ipcompTransformEntry 9 }

--
-- IKE endpoint 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 ollection of IPProtocolEndpoints) to identify itself in IKE phase 1 negotiations. The column .UseIKEIdentityType in an ikeActionEntry specifies which type of the available identities to use in a negotiation exchange and the column. IdentityContexts in an ikeRule specifies the match values to be used, along with the local address, to be used in selecting the appropriate identity for a negotiation. The ElementID property value should be that of either the IPProtocolEndpoint

or Collection of endpoints as appropriate."
 ::= { ipsecPolicyConfigObjects 23 }

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

IkeIdentityEntry ::= SEQUENCE {
ikeIdentityType IpsecDoiIdentType,
ikeIdentityIdString OCTET STRING,
ikeIdentityIsOriginator INTEGER,

Various Authors

[Page 69]

Internet Draft

IPsec Policy Configuration MIB

November 2001

ikeIdentityLastChanged TimeStamp,
ikeIdentityStorageType StorageType,
ikeIdentityRowStatus RowStatus
}

ikeIdentityType OBJECT-TYPE
SYNTAX IpsecDoiIdentType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The IdentityType specifies the type of IKE Identity."
 ::= { ikeIdentityEntry 1 }

ikeIdentityIdString OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"Identity 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 2 }

ikeIdentityIsOriginator OBJECT-TYPE
SYNTAX INTEGER { originator(1), nonOriginator(2) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object specifies whether the local IKE entity will initiate the IKE negotiation with this peer when such action is triggered by a non-traffic driven event."
 ::= { ikeIdentityEntry 3 }

ikeIdentityLastChanged 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 }

ikeIdentityStorageType 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 }
 ::= { ikeIdentityEntry 5 }

ikeIdentityRowStatus 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.


```
XXX: indicate minimum conditions allowed when transitioning
      between non-active and active states (both directions). IE,
      which sub/super-table rows must be of the requested stated?
      Which columns must be defined for this row to be operational?"
 ::= { ikeIdentityEntry 6 }
```

```
--
-- Shared Secrets Table
--
```

```
sharedSecretsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SharedSecretsTableEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of shared secret values."
    ::= { ipsecPolicyConfigObjects 24 }
```

```
sharedSecretsTableEntry OBJECT-TYPE
    SYNTAX      SharedSecretsTableEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        ""
    INDEX      { sstName }
    ::= { sharedSecretsTable 1 }
```

```
SharedSecretsTableEntry ::= SEQUENCE {
    sstName                SnmpAdminString,
    sstRemoteID            OCTET STRING,
    sstSecret              OCTET STRING,
    sstPasswordAlgorithm  OCTET STRING,
    sstLastChanged        TimeStamp,
    sstStorageType        StorageType,
    sstRowStatus           RowStatus
}
```

```
sstName 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."
 ::= { sharedSecretsTableEntry 1 }

sstRemoteID 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 shared secret on the remote site. If there is no ID associated with this secret, the value of this object should be the null string."
 ::= { sharedSecretsTableEntry 2 }

sstSecret OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object represents the secret (e.g. key) value. When accessed for reading, it MUST return a null length (0 length) string and MUST NOT return the configured secret."
 ::= { sharedSecretsTableEntry 3 }

sstPasswordAlgorithm OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object represents the transformation algorithm used to protect passwords before use in the protocol. For shared secrets without a password, this value can be ignored. For shared secrets that have passwords but no transform algorithm,

 this object should be the null string."
 ::= { sharedSecretsTableEntry 4 }

sstLastChanged 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."
 ::= { sharedSecretsTableEntry 5 }

sstStorageType 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."
 ::= { sharedSecretsTableEntry 6 }

sstRowStatus 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.

 XXX: indicate minimum conditions allowed when transitioning
 between non-active and active states (both directions). IE,
 which sub/super-table rows must be of the requested stated?
 Which columns must be defined for this row to be operational?"
 ::= { sharedSecretsTableEntry 7 }

END

[6. Security Considerations](#)

[6.1 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.

[6.2](#) 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.

[6.3](#) 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.

[6.4](#) 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.

[7.](#) Author's 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
Redcreek Communications
3900 Newpark Mall Rd.
Newark, CA 94560
Phone: +1 510 795 6903
Email: rcharlet@redcreek.com

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

Jon Saperia

Various Authors

[Page 75]

Internet Draft

IPsec Policy Configuration MIB

November 2001

JDS Consulting, Inc.
174 Chapman Street
Watertown, MA 02472
Phone: +1 617 744 1079
Email: saperia@jdscons.com

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

8. 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.

Various Authors

[Page 76]

Internet Draft

IPsec Policy Configuration MIB

November 2001

[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, "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-ipsip-config-policy-model-02.txt](#), March 2001.

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.

[10](#). Full Copyright Statement

Copyright (C) The Internet Society (2001). 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.