

IPSP Working Group
Internet Draft
[draft-ietf-ipsec-conf-mib-00.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
Feb 2001

IPsec Policy Configuration MIB
draft-ietf-ipsec-conf-mib-00.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/1id-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/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 IPsec/IKE devices. 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](#) [1].
- 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](#) [2], STD 16, [RFC 1212](#) [3] and [RFC 1215](#) [4]. The second version, called SMIV2, is described in STD 58, [RFC 2578](#) [5], [RFC 2579](#) [6] and [RFC 2580](#) [7].
- 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](#) [8]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in [RFC 1901](#) [9] and [RFC 1906](#) [10]. The third version of the message protocol is called SNMPv3 and described in [RFC 1906](#) [10], [RFC 2572](#) [11] and [RFC 2574](#) [12].
- o Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is described in STD 15, [RFC 1157](#) [8]. A second set of protocol operations and associated PDU formats is described in [RFC 1905](#) [13].
- o A set of fundamental applications described in [RFC 2573](#) [14] and the view-based access control mechanism described in [RFC 2575](#) [15].

A more detailed introduction to the current SNMP Management Framework can be found in [RFC 2570](#) [18].

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

This memo specifies a MIB module that is compliant to the SMIV2. A

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

3. Relationship to the DMTF Policy Model

The Distributed Management Task Force has created an object oriented model of IPsec policy information known as the IPsec Policy Model White Paper. The contents of this document are also reflected in the internet draft "IPsec Configuration Policy Model" (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 You can't implement groups of groups of policies with this MIB. There can however be multiple groups associated with an IpProtocolEndpoint (an interface). We felt this was simpler to represent in SMI and accomplishes the same goals.
- o There can be a list of actions and a list of fall-back actions associated with a condition set via one rule. The list of actions is intended to accommodate performing both multiple actions as well as actions aside from IPsec on packets matching this condition set (like NAT or QOS...). The list of fall-back actions is intended to accommodate IKE redundancy incase an IKE peer is unreachable.
- o The various filter objects were combined into a single table and hence multiple filters can be represented in one row of an SMI table. This promotes efficiency of data storage since some information can be shared in circumstances where this is

appropriate to make use of.

- o Conditions were modified to be of more than one type, rather than being forced to be triggered only during one event type. This allows them to be configured to be, for example, both a

startup condition and a manually activated condition.

4. Elements of Procedure

This section describes the elements of procedure that a security policy database engine would follow when processing an event using the

rules defined by the IPSEC-POLICY-MIB. An event that triggers processing using this data would be one of:

- 1) startup of the engine.
- 2) a manual administrative request to process a rule.
- 3) unprotected data arriving across an endpoint.
- 4) an IKE message arriving across an endpoint.

The steps to be taken when one of these events occurs are:

- 1) Consult the `policyEndpointToGroupTable` using the endpoint's transport domain and address as indexes to the table. An ordered list of groups (G) referenced by the `peGroupName` object are extracted from the `policyEndpointToGroupTable` table and are ordered according to the `peEndpointPriority` column, the lowest of the `peEndpointPriority` values being processed first.
- 2) For each group in (G), the `policyIKERulesInGroupTable` and the `policyIPsecRulesInGroupTable` are consulted using the `peGroupName` as an index to produce an ordered (using `policyIKERulePriority` and `policyIPsecRulePriority`) list of IKE Rules (I) and IPsec rules (R).
- 3) Each of the rules in (I) and (R) are then processed to determine if they are applicable by consulting the `conditionsInRuleTable` table to produce an ordered (using `conditionSequenceNumber`) list of conditions (C).
- 4) For each condition, the `conditionUsage` object in the `conditionTable` is first consulted to see if the condition is viable for the event in question. If it is viable for the given event and the event involves traffic, a list of filters (F) for the condition is extracted from the `filtersInConditionTable`.
- 5) Each filter in (F) is evaluated to determine if it is true or false. Multiple tests defined inside a filter must all pass for the filter to be true. Filters that are to be applied to both

the source and destination addresses, as defined by the
ficOnDestination object, must be run twice and be successful on
each address in order to be considered successful itself. The result
is possibly negated, based on the value of the ficFilterIsNegated
object in the filtersInConditionTable.

- 6) If any filter fails to pass any of its tests, the entire condition is considered to have failed. Note that the result of the condition is possibly negated according to the conditionIsNegated object in the conditionsInRuleTable. Based on the final result of this condition, one of the following should be performed:
- a) If the final result of the condition is false, and the pgIKEConditionListType for the current rule is 'and' then the next rule must be processed, returning to step #3.
 - b) If the condition is false and the pgIKEConditionListType type is 'or', then the next condition in (C) must be processed, returning to step #4, unless no further rules exist in (I) or (R) in which case the next group in (G) must be processed by returning to step #2, unless there are no further groups in (G), in which case the current packet must be dropped and this action possibly logged (according to XXX).
 - c) If the condition result is true and the pgIKEConditionListType is 'and' then the next condition in (C) must be processed, returning to step #4, unless it is the last condition in (C) in which case the rule is considered to have passed its conditions and step #7 should be consulted.
 - d) If the condition result is true and the pgIKEConditionListType is 'or' then processing of the conditions in (C) and the rule is considered to have passed its conditions and step #7 should be consulted.
- 7) Using the actionRuleName, the actionsInRuleTable should be consulted to retrieve a list of ordered actions. This list is constructed by consulting the table where the lowest actionFailureSequenceNumber associated with the actionRuleName is taken and all rows matching both the actionRuleName and this value of the actionFailureSequenceNumber are collected and prioritized according to the actionSuccessSequenceNumber object. This should produce an initial set of actions (A).
- 8) Each action in (A) is executed according to the parameters

associated with it according to the value of the actionName
RowPointer, which should be a pointer into a table which
describes
what action should be taken and what parameters are to be used
when
executing it. The two action tables defined in this MIB for use
with this row pointer are the saStaticActionTable and the
saNegotiationActionTable.

- 9) Depending on whether all the actions in (A) succeed or fail, the following steps must be taken:

- a) If any action in (A) fails, a new set (A) is constructed using the next highest value of actionFailureSequenceNumber, returning to step 8 to execute them (functionally, these are "fall-back actions"). If no further fall-back actions exist in the actionsInRuleTable, then processing of the current packet must be halted and the packet is dropped. This event should be logged (XXX: define notifications).
- b) If all of the actions in (A) succeed, then processing of this packet stops (IE, no further groups or rules are consulted).

5. Definitions

IPSEC-POLICY-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-IDENTITY, OBJECT-TYPE, Integer32,
 Unsigned32 FROM SNMPv2-SMI
 TEXTUAL-CONVENTION, RowStatus, TruthValue,
 TimeStamp, StorageType, RowPointer,
 TDomain, TAddress FROM SNMPv2-TC
 MODULE-COMPLIANCE, OBJECT-GROUP
 NOTIFICATION-GROUP FROM SNMPv2-CONF
 SnmpAdminString FROM

SNMP-FRAMEWORK-MIB;

--

-- 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.

Various Authors

[Page 6]

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

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

XXX: insert everyone else's"

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."
::= { XXX }

--
-- 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 TruthValue

IpsecGroupId ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"The IpsecGroupId specifies the Diffie-Hellman group to use for phase 2 negotiations. A vendor specific GroupID range is available for use from 32768-65535. The well known groupIDs defined here are taken from [RFC2412](#)."

SYNTAX INTEGER { modp768(1), modp1024(2), ec2ngp155(3), ec2ngp185(4), modp1536(5) }

--

-- Policy group definitions

--

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 that they will apply to. Any policy groups assigned to this endpoint are then used to control access to the traffic passing by it.

If an endpoint has been configured with at least one policy group and no contained rule in any group matched the incoming packet, the default action in this case shall be to drop the packet.

If no policy groups have 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.

The peGroupPriority object indicates the ordering that a list of groups will be applied to a given endpoint. Once a group 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 by finding the next largest peGroupPriority object shall only be done if no actions were run when processing the last group

for

a given packet."

::= { ipsecPolicyConfigObjects 1 }

policyEndpointToGroupEntry OBJECT-TYPE
SYNTAX PolicyEndpointToGroupEntry
MAX-ACCESS not-accessible

```
STATUS      current
DESCRIPTION
    "A mapping assigning a policy group to an endpoint."
INDEX       { peEndpointDomain, peEndpointAddress, peGroupPriority
}
 ::= { policyEndpointToGroupTable 1 }

PolicyEndpointToGroupEntry ::= SEQUENCE {
    peEndpointDomain      TDomain,
    peEndpointAddress     TAddress,
    peGroupPriority       Integer32,
    peGroupName           SnmpAdminString,
    peLastChanged         TimeStamp,
    peStorageType         StorageType
}

peEndpointDomain OBJECT-TYPE
    SYNTAX      TDomain
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The TDomain 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."
    ::= { policyEndpointToGroupEntry 1 }

peEndpointAddress OBJECT-TYPE
    SYNTAX      TAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The address of a given endpoint, the format of which is
        specified by the peEndpointDomain object."
    ::= { policyEndpointToGroupEntry 2 }

peGroupPriority OBJECT-TYPE
    SYNTAX      Integer32 (1..65536)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A number specifying the priority level of this group.  A
        group assigned to an endpoint with a lower numerical priority
        level is processed before a group assigned to the same
        endpoint with a higher numerical priority level.  Processing
        of groups on an endpoint stops as soon after the first action
        in a group is executed."
```

```
::= { policyEndpointToGroupEntry 3 }
```

peGroupName OBJECT-TYPE

SYNTAX SnmpAdminString

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 policyIKERulesInGroupTable and the policyIPsecRulesInGroupTable to come up with a list of rules that MUST be applied to this endpoint."

::= { policyEndpointToGroupEntry 4 }

peLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-create

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 5 }

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 6 }

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.

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?"

```
 ::= { policyEndpointToGroupEntry 7 }
```

```
--
```

```
-- Policy IKE Rules in a Group Table
```

```
--
```

```
policyIKERulesInGroupTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF PolicyIKERulesInGroupEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"This table holds a listing of IKE rules. Conditions and
Actions are associated with each rule in this table through
the conditionsInRuleTable and actionsInRuleTable
```

```
respectively.
```

```
"
```

```
 ::= { ipsecPolicyConfigObjects 2 }
```

```
policyIKERulesInGroupEntry OBJECT-TYPE
```

```
SYNTAX PolicyIKERulesInGroupEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"A particular IKE rule associated with a policy group."
```

```
INDEX { peGroupName, pgIKERulePriority }
```

```
 ::= { policyIKERulesInGroupTable 1 }
```

```
PolicyIKERulesInGroupEntry ::= SEQUENCE {
```

```
pgIKERulePriority Integer32,
```

```
pgIKERuleName SnmpAdminString,
```

```
pgIKERuleDescription OCTET STRING,
```

```
pgIKEConditionListType IpsecBooleanOperator,
```

```
pgIKEidentityContexts OCTET STRING,
```

```
pgIKERuleLastChanged TimeStamp,
```

```
pgIKERuleStorageType StorageType
```

```
}
```

```
pgIKERulePriority OBJECT-TYPE
```

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

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

```
STATUS current
```

```
DESCRIPTION
```

```
"pgIKERulePriority is the priority of this pgIKERuleName
within its relevant peGroupName. This represents the order
that Rules should be processed within Groups. Lower values
are processed first."
```

```
 ::= { policyIKERulesInGroupEntry 1 }
```

pgIKERuleName OBJECT-TYPE

Various Authors

[Page 11]

```
SYNTAX      SnmpAdminString
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "pgIKERuleName is the name of the rule associated with a
    pgGroupName. This name will match a set of
    conditionsInRuleEntries and a set of actionsInRuleEntries via
    the contitionRuleName and actionRuleName respectively. Those
    are the conditions and actions associated with this rule."
 ::= { policyIKERulesInGroupEntry 2 }
```

pgIKERuleDescription 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' }
 ::= { policyIKERulesInGroupEntry 3 }
```

pgIKEConditionListType OBJECT-TYPE

```
SYNTAX      IpsecBooleanOperator
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "pgIKEConditionListType defines if the list of associated
    conditions with this rule is an ANDED list or an ORed list."
DEFVAL { true }
 ::= { policyIKERulesInGroupEntry 4 }
```

pgIKEidentityContexts OBJECT-TYPE

```
SYNTAX      OCTET STRING (SIZE(0..511))
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "pgIKEidentityContexts is a string array that corresponds to
    an ANDED list of values. If the string is broken by a CR LF
    sequence, then multiple strings exist, and they are to be
    logically ORed with each other. 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."
 ::= { policyIKERulesInGroupEntry 5 }
```

pgIKERuleLastChanged OBJECT-TYPE


```
SYNTAX      TimeStamp
MAX-ACCESS  read-create
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."
 ::= { policyIKERulesInGroupEntry 6 }
```

```
pgIKERuleStorageType OBJECT-TYPE
```

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

```
    "The storage type for this row.  Rows in this table which were
of
    created through an external process may have a storage type
    readOnly or permanent.  Entries which are permanent are
but
    expected to have at least one configurable column in the row,
    which columns are in fact modifiable is implementation
specific."
    DEFVAL { nonVolatile }
 ::= { policyIKERulesInGroupEntry 7 }
```

```
pgIKERuleRowStatus 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?"
 ::= { policyIKERulesInGroupEntry 8 }
```

```
--
-- Policy IPsec Rules in a Group Table
--
```

```
policyIpsecRulesInGroupTable OBJECT-TYPE
```

```
SYNTAX      SEQUENCE OF PolicyIpsecRulesInGroupEntry
```

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This table holds lists of IpsecRules associated with
pePolicyGroups. Each peGroupName may have a list of

policyIpsecRules associated with it. Each policyIpsecRule may in turn have a list of conditions and actions associated with it."

::= { ipsecPolicyConfigObjects 3 }

policyIpsecRulesInGroupEntry OBJECT-TYPE

SYNTAX PolicyIpsecRulesInGroupEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A particular IPsec Rule associated with a policy group."

INDEX { pgGroupName, pgIPsecRulePriority }

::= { policyIpsecRulesInGroupTable 1 }

PolicyIpsecRulesInGroupEntry ::= SEQUENCE {

pgIPsecRulePriority	Integer32,
pgIPsecRuleName	SnmpAdminString,
pgIPsecRuleDescription	OCTET STRING,
pgIPsecConditionListType	IpsecBooleanOperator,
pgIPsecRuleLastChanged	TimeStamp,
pgIPsecRuleStorageType	StorageType

}

pgIPsecRulePriority OBJECT-TYPE

SYNTAX Integer32 (1..65536)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"pgIPsecRulePriority is the priority of this pgIPsecRuleName within its relevant pgGroupName. This represents the order that Rules should be processed within Groups. Lower values are processed first."

::= { policyIpsecRulesInGroupEntry 1 }

pgIPsecRuleName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"pgIPsecRuleName is the name of the rule associated with a pgGroupName. This name will match a set of conditionsInRuleEntries and a set of actionsInRuleEntries via the conditionRuleName and actionRuleName respectively. Those are the conditions and actions associated with this rule."

::= { policyIpsecRulesInGroupEntry 2 }

pgIPsecRuleDescription 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 }
 ::= { policyIpsecRulesInGroupEntry 3 }
```

```
pgIPsecConditionListType OBJECT-TYPE
SYNTAX IpsecBooleanOperator
MAX-ACCESS read-create
STATUS current
DESCRIPTION
    "pgIPsecConditionListType defines if the list of associated
    conditions with this rule is an ANDed list or an ORed list."
DEFVAL { true }
 ::= { policyIpsecRulesInGroupEntry 4 }
```

```
pgIPsecRuleLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-create
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."
 ::= { policyIpsecRulesInGroupEntry 5 }
```

```
pgIPsecRuleStorageType 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 }
 ::= { policyIpsecRulesInGroupEntry 6 }
```

```
pgIPsecRuleRowStatus 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?"

```
 ::= { policyIpsecRulesInGroupEntry 7 }
```

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

conditionsInRuleTable OBJECT-TYPE

SYNTAX SEQUENCE OF ConditionsInRuleEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The table of conditions associated with an ipsec policy rule. In particular, an pgIPsecRuleName can be used to get a list of related conditionName's and their parameters from this

table."

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

conditionsInRuleEntry OBJECT-TYPE

SYNTAX ConditionsInRuleEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"conditionsInRuleEntry represents a condition associated with rule."

INDEX { conditionRuleName, conditionSequenceNumber }

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

ConditionsInRuleEntry ::= SEQUENCE {

conditionRuleName SnmpAdminString,

conditionSequenceNumber Integer32,

conditionIsNegated IpsecIsNegated,

conditionName SnmpAdminString,

conditionLastChanged TimeStamp,

conditionStorageType StorageType

}

conditionRuleName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

```
"conditionRuleName is the name of the rule that is associated  
with conditionName"  
::= { conditionsInRuleEntry 1 }
```

conditionSequenceNumber OBJECT-TYPE

SYNTAX Integer32 (1..65536)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

in "conditionSequenceNumber is the priority of the conditionName
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

STATUS current

DESCRIPTION

the "conditionIsNegated indicates whether the condition results
should be negated (e.g. if a boolean 'not' is performed on
condition)."
DEFVAL { false }
::= { conditionsInRuleEntry 3 }

conditionName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-create

STATUS current

DESCRIPTION

the "conditionName is the name of the condition associated with
conditionRuleName."
::= { conditionsInRuleEntry 4 }

conditionLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-create

STATUS current

DESCRIPTION

created "The value of sysUpTime when this row was last modified or
either through SNMP SETs or by some other external means."
::= { conditionsInRuleEntry 5 }

conditionStorageType 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 }
```

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.

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 }
```

--

-- Policy Actions in a rule table

--

actionsInRuleTable OBJECT-TYPE

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

DESCRIPTION

"This table of actions associates actions with an ipsec policy rule.

In Particular, an pgIPsecRuleName can be used to get a list of related actionName's from this table. This table can

includes

multiple actions that are associated with a rule name and any fallback actions associated with that rule name."

```
 ::= { ipsecPolicyConfigObjects 5 }
```

actionsInRuleEntry OBJECT-TYPE

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

DESCRIPTION

"actionsInRuleEntry represents an action associated with a rule."

```
INDEX      { actionRuleName, actionFailureSequenceNumber,  
            actionSuccessSequenceNumber }
```

```
::= { actionsInRuleTable 1 }
```

```
ActionsInRuleEntry ::= SEQUENCE {  
    actionRuleName                SnmpAdminString,  
    actionFailureSequenceNumber   Integer32,  
    actionSuccessSequenceNumber   Integer32,  
    actionName                     RowPointer,  
    actionLastChanged              TimeStamp,  
    actionStorageType              StorageType  
}
```

```
actionRuleName OBJECT-TYPE
```

```
SYNTAX      SnmpAdminString
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "actionRuleName is the name of the rule that is associated
```

```
with
```

```
    actionName."
```

```
::= { actionsInRuleEntry 1 }
```

```
actionFailureSequenceNumber OBJECT-TYPE
```

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

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "actionFailureSequenceNumber represents the ordering of
```

```
fallback
```

```
    actions. Lower numbers indicate action sets that are  
    attempted first. e.g. if the actions with the same value of  
    actionRuleName and actionFailureSequenceNumber fail, the  
    actions (if any) with the same actionRuleName but with the  
    next higher value of actionFailureSequenceNumber will be  
    attempted next."
```

```
::= { actionsInRuleEntry 2 }
```

```
actionSuccessSequenceNumber OBJECT-TYPE
```

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

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "actionSuccessSequenceNumber represents the ordering of
```

```
actions
```

```
    associated with a rule. Lower numbers indicate actions that
```

```
are
```

```
    attempted first. The group of rows that have the same  
    actionRuleName and actionFailureSequenceNumber indicate (by  
    actionName) the actions that should be completed in the order
```

```
        specified by actionSuccessSequenceNumber."  
 ::= { actionsInRuleEntry 3 }
```

actionName OBJECT-TYPE

SYNTAX RowPointer
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"actionName is the name of the action that is associated with
actionRuleName."
::= { actionsInRuleEntry 4 }

actionLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-create
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."
::= { actionsInRuleEntry 5 }

actionStorageType 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 }
::= { actionsInRuleEntry 6 }

actionRowStatus 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 actionsInRuleTable to change to the active
state,
the row in the
XXX: actionTable?"

indicated by actionName must be active and the row in the
XXX: rowTable/saRowTable?
indicated by actionRuleName must be active.
No conditions are necessary to become inactive, although the
rows in

```

        XXX: actionTable? and rowTable/saRowTable?
        should be active at all times that this row is active.  "
 ::= { actionsInRuleEntry 7 }

--
-- 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 6 }

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,
    conditionLastChanged     TimeStamp,
    conditionStorageType     StorageType
}

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 }
```

```
conditionLastChanged OBJECT-TYPE
```

```
SYNTAX      TimeStamp
```

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

```
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 3 }
```

```
conditionStorageType 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 }
```

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

```
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 5 }

--
--
--

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 7 }

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 ficFilterName which can be used as an index into the filterTable to retrieve the filter's definition."

INDEX { conditionName, ficFilterName }

::= { filtersInConditionTable 1 }

FiltersInConditionEntry ::= SEQUENCE {

ficFilterName SnmpAdminString,

ficOnDestination BITS,

ficLastChanged TimeStamp,

ficStorageType StorageType

}

ficFilterName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An administratively assigned unique name that can be used to reference the filter's definition via the filterTable."

::= { filtersInConditionEntry 1 }

ficOnDestination OBJECT-TYPE

SYNTAX BITS { source(0), destination(1) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Whether the filter is to be applied to the source and/or the destination address. If both the source and destination

address bits are set, the filter must successfully apply to both addresses for the filter itself to be considered to have successful result."

::= { filtersInConditionEntry 2 }

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 { false }

::= { filtersInConditionEntry 3 }

ficLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-create

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 4 }

ficStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

of

readOnly or permanent. Entries which are permanent are expected to have at least one configurable column in the row,

but

which columns are in fact modifiable is implementation

specific."

DEFVAL { nonVolatile }

::= { filtersInConditionEntry 5 }

ficRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

The value of this object has no effect on whether other

objects in this conceptual row can be modified.

This object can not be made active until the filter
referenced
by the ficFilterName 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 6 }
```

```
--
```

```
-- 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 8 }
```

```
filterEntry OBJECT-TYPE
```

```
SYNTAX FilterEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"A particular filter definition. For a filter to be  
considered to have a TRUE result, all of the tests as defined  
by the filterType column must pass successfully. In other  
words, all sub-tests of a given filter are logically ANDed  
together."
```

```
INDEX { ficFilterName }
```

```
::= { filterTable 1 }
```

```
FilterEntry ::= SEQUENCE {
```

```
filterType BITS,  
filterExternalOID OBJECT IDENTIFIER,  
filterDomain TDomain,  
filterAddress TAddress,  
filterMask TAddress,
```

filterRangeBegin
filterRangeEnd
filterFQDNName

TAddress,
TAddress,
OCTET STRING,

```

    filterClassificationLevel      Integer32,
    filterAuthority                 Integer32,
    filterLastChanged              TimeStamp,
    filterStorageType              StorageType
  }

```

filterType OBJECT-TYPE

```

  SYNTAX      BITS { external(0), addressOrNetwork(1),
addressRange(2),
              fqdn(3), protocol(4), portRange(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.

tests

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 filterDomain, filterAddress and filterMask objects. Any protocol and/or port specification defined by the filterDomain object is ignored for this test and only the address related information is used from the

filterAddress

and filterMask objects to evaluate this test.

A row with a filterRowStatus object set to active may not have the addressOrNetwork test bit turned on until either

the

filterRowStatus value is changed to notInService or until the filterDomain, filterAddress, and filterMask objects have been appropriately configured first. Attempting to do so will produce a inconsistentValue error.

A row in this table which is not active and with the addressOrNetwork test bit set will cause the filterRowStatus object to return the notReady state if

the `filterDomain`, `filterAddress`, and `filterMask` objects have not been appropriately configured.

`addressRange`:

- Tests to see if an address falls within a starting and

ending address pair using the filterRangeBegin and filterRangeEnd objects. Any protocol and/or port specification defined by the filterDomain object is ignored for this test and only the address related information is used from the filterRangeBegin and filterRangeEnd objects to evaluate this test.

A row with a filterRowStatus object set to active may not have the addressRange test bit turned on until either the filterRowStatus value is changed to notInService or until the filterDomain, filterRangeBegin, and filterRangeEnd objects have been appropriately configured first. Attempting to do so will produce a inconsistentValue error.

A row in this table which is not active and with the addressRange test bit set will cause the filterRowStatus object to return the notReady state if the filterDomain, filterRangeBegin, and filterRangeEnd objects have not been appropriately configured.

fqdn:

- Tests to see if an address matches a fully-qualified-domain-name expression defined by the filterFQDNName object. The filterFQDNName object may contain a string that will match a single host, such as host.company.com, or may contain an expression using wildcards such as *.company.com.

A row with a filterRowStatus object set to active may not have the fqdn test bit turned on until either the filterRowStatus value is changed to notInService or until the filterFQDNName object has been appropriately configured first. Attempting to do so will produce a inconsistentValue error.

A row in this table which is not active and with the fqdn test bit set will cause the filterRowStatus object to return the notReady state if the filterFQDNName object

has

not been appropriately configured.

protocol:

- Tests to see if the incoming packet matches the protocol as defined by the filterDomain object. The other aspects of the filterDomain object (address and port information) are ignored when evaluating this test.

A row with a `filterRowStatus` object set to active may not

have the protocol test bit turned on until either the filterRowStatus value is changed to notInService or until the filterDomain object has been appropriately configured first. Attempting to do so will produce a inconsistentValue error.

A row in this table which is not active and with the protocol test bit set will cause the filterRowStatus object to return the notReady state if the filterDomain 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 filterRangeBegin and filterRangeEnd objects. Any protocol and/or address specification defined by the filterDomain object is ignored for this test and only the port number related information is used from the filterRangeBegin and filterRangeEnd objects to evaluate this test. If the protocol specified by the filterDomain object does not contain port number information, the result of this test will be false.

XXX: disallow setting filterDomain to a domain that doesn't contain a port range if the portRange test is specified?

A row with a filterRowStatus object set to active may not have the portRange test bit turned on until either the filterRowStatus value is changed to notInService or until the filterDomain, filterRangeBegin, and filterRangeEnd objects have been appropriately configured first. Attempting to do so will produce a inconsistentValue error.

A row in this table which is not active and with the portRange test bit set will cause the filterRowStatus object to return the notReady state if the filterDomain, filterRangeBegin, and filterRangeEnd objects have not been appropriately configured.

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 with a filterRowStatus object set to active may not have the classification test bit turned on until either the filterRowStatus value is changed to notInService or until the filterClassificationLevel object has been appropriately configured first. Attempting to do so will produce a inconsistentValue error.

A row in this table which is not active and with the classification test bit set 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 with a filterRowStatus object set to active may not have the authority test bit turned on until either the filterRowStatus value is changed to notInService or until the filterAuthority object has been appropriately configured first. Attempting to do so will produce a inconsistentValue error.

A row in this table which is not active and with the authority test bit set will cause the filterRowStatus object to return the notReady state if the filterAuthority object has not been appropriately configured.

XXX: is an empty test set legal? if so, is it true or false?
"

::= { filterEntry 1 }

filterExternalOID OBJECT-TYPE

SYNTAX OBJECT IDENTIFIER

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"XXX: To be defined later."

::= { filterEntry 2 }

filterDomain OBJECT-TYPE

SYNTAX

TDomain

Various Authors

[Page 30]

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.

a For the portRange test, if the filterDomain does not specify 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 3 }

filterAddress OBJECT-TYPE
 SYNTAX TAddress
 MAX-ACCESS read-create
 STATUS current
 DESCRIPTION

"The address to use when performing an addressOrNetwork test.

filterMask For an addressOrNetwork test, the filterAddress and 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 4 }

filterMask OBJECT-TYPE
 SYNTAX TAddress
 MAX-ACCESS read-create
 STATUS current
 DESCRIPTION

"The network mask to use when performing an addressOrNetwork

test. This mask will be applied to the filterAddress object contents to produce a subnet address to test against. A network mask consisting of all bits set to 1 should be used when an exact match against the entire address from the filterAddress is desired.

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 }
```

filterRangeBegin OBJECT-TYPE

SYNTAX TAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Defines the beginning half of an address and/or port range to be used when performing addressRange or portRange tests.

The addressRange test is considered a success if and only if the address type specified by the filterDomain object matches the address type of the address to be tested against AND the address to be tested against falls between the addresses defined in the filterRangeBegin and filterRangeEnd objects. If a port and/or protocol is specified by this object or the filterDomain object, it is ignored for the purpose of this

test.

The portRange test is considered a success if and only if the port number to be tested against falls between the port numbers specified in the filterRangeBegin and filterRangeEnd objects. This test is to be considered a failure if the filterRangeBegin/filterRangeEnd objects don't include a port number because the filterDomain object doesn't specify a TAddress type that requires one. If an address and/or protocol is specified by this object or the filterDomain object, it is ignored for the purpose of this test."

```
::= { filterEntry 6 }
```

filterRangeEnd OBJECT-TYPE

SYNTAX TAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Defines the ending half of an address and/or port range to be used when performing addressRange or portRange tests."

```
::= { filterEntry 7 }
```

filterFQDNName OBJECT-TYPE

Various Authors

[Page 32]

```
SYNTAX      OCTET STRING
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "Defines a string used to match against the host name of the
    packet to be filtered.  The string may contain one or more
    wildcard characters '*', so as to match an entire domain such
    as '*.mydomain.com'."
 ::= { 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-create
    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.

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 if the requirements of
the filterType object are not meant. 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.

Once a row in this table has been made active by this object,
the value of this object for that row MAY NOT be changed
(E.G., to destroy or notInService) if any active row in the
filtersInConditionTable table has it's ficFilterName object
set to this row's ficFilterName. An attempt to do so will
result in an inconsistentValue error.

A row in this table which is not active and with the
addressOrNetwork test bit set will cause the filterRowStatus
object to return the notReady state if the filterDomain,
filterAddress, and filterMask objects have not been
appropriately configured.

A row in this table which is not active and with the
addressRange test bit set will cause the filterRowStatus
object to return the notReady state if the filterDomain,
filterRangeEnd, and filterRangeEnd objects have not been
appropriately configured.

test
A row in this table which is not active and with the fqdn

bit set will cause the filterRowStatus object to return the
notReady state if the filterFQDNName object has not been
appropriately configured.

A row in this table which is not active and with the protocol test bit set will cause the filterRowStatus object to return

the notReady state if the filterDomain object has not been appropriately configured.

A row in this table which is not active and with the portRange test bit set will cause the filterRowStatus object to return the notReady state if the filterDomain, filterRangeEnd, and filterRangeEnd objects have not been appropriately configured.

A row in this table which is not active and with the classification test bit set will cause the filterRowStatus object to return the notReady state if the filterClassificationLevel object has not been appropriately configured.

A row in this table which is not active and with the authority test bit set will cause the filterRowStatus object to return the notReady state if the filterAuthority object has not been appropriately configured.

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?"

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

```
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 9 }
```

```
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,  
    sasActionLifetime      Integer32,
```

```
    sasDoLogging           TruthValue,
    sasLastChanged         TimeStamp,
    sasStorageType         StorageType
}
```

sasActionName OBJECT-TYPE

```
SYNTAX      SnmpAdminString
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),
preconfigured(3) }
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

3 ----- use the pre-configured SA."

```
::= { saStaticActionEntry 3 }
```

sasActionLifetime OBJECT-TYPE

```
SYNTAX      Integer32
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
```

"sasActionLifetime specifies how long the security association derived from this action should be used."

```
::= { saStaticActionEntry 4 }
```

sasDoLogging OBJECT-TYPE

SYNTAX

TruthValue

Various Authors

[Page 36]

MAX-ACCESS read-create
STATUS current
DESCRIPTION

"sasDoLogging specifies whether or not an audit message should be logged when a packet is discarded."

::= { saStaticActionEntry 5 }

sasLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-create
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 6 }

sasStorageType 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 }
::= { saStaticActionEntry 7 }

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 8 }
```

saNegotiationActionTable OBJECT-TYPE

```

SYNTAX      SEQUENCE OF SaNegotiationActionEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "This table lists all the possible IPsec and IKE actions."
 ::= { ipsecPolicyConfigObjects 10 }

```

```

saNegotiationActionEntry OBJECT-TYPE
SYNTAX      SaNegotiationActionEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "Contains the attributes of one saNegotiationActionEntry."
INDEX       { sanActionName }
 ::= { saNegotiationActionTable 1 }

```

```

SaNegotiationActionEntry ::= SEQUENCE {
    sanActionName                SnmpAdminString,
    sanActionDescription          OCTET STRING,
    sanIKEActionName             SnmpAdminString,
    sanIPsecActionName           SnmpAdminString,
    sanMinimumLifetimeSeconds    Integer32,
    sanMinimumLifetimeKB         Integer32,
    sanRefreshThresholdSeconds   Integer32,
    sanRefreshThresholdKB        Integer32,
    sanIdleDurationSeconds       Integer32,
    sanLastChanged               TimeStamp,
    sanStorageType               StorageType
}

```

```

sanActionName OBJECT-TYPE
SYNTAX      SnmpAdminString
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "This object contains the name of this
SaNegotiationActionEntry.
This row
    can be referred to by an actionsInRuleEntry"
 ::= { saNegotiationActionEntry 1 }

```

```

sanActionDescription 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' }

```
::= { saNegotiationActionEntry 2 }
```

```
sanIKEActionName OBJECT-TYPE
```

```
SYNTAX      SnmpAdminString
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "This row will refer to an IkeActionEntry of the  
ikeActionTable."
```

```
::= { saNegotiationActionEntry 3 }
```

```
sanIPsecActionName OBJECT-TYPE
```

```
SYNTAX      SnmpAdminString
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "This row will refer to an IpsecActionEntry of the  
ipsecActionTable."
```

```
::= { saNegotiationActionEntry 4 }
```

```
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."
```

```
::= { saNegotiationActionEntry 5 }
```

```
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."
```

```
::= { saNegotiationActionEntry 6 }
```

```
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."

::= { saNegotiationActionEntry 7 }

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."

::= { saNegotiationActionEntry 8 }

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."

::= { saNegotiationActionEntry 9 }

sanLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-create

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."

::= { saNegotiationActionEntry 10 }

sanStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

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

```
DEFVAL { nonVolatile }
 ::= { saNegotiationActionEntry 11 }
```

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.

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?"

```
::= { saNegotiationActionEntry 12 }
```

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."

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

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,
ikeThresholdDerivedKeys Integer32,
```

ikeExchangeMode
ikeAgressiveModeGroupId
ikeProposalName
ikeEndpointName

INTEGER,
IpsecGroupId,
SnmpAdminString,
SnmpAdminString,

```
    ikeActionLastChange          TimeStamp,
    ikeActionStorageType        StorageType
}
```

ikeActionName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

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

row

will be referred to by an SaNegotiationActionEntry."

::= { ikeActionEntry 1 }

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 2 }

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 3 }

ikeAggressiveModeGroupId OBJECT-TYPE

SYNTAX IpsecGroupId

MAX-ACCESS read-create

STATUS current

DESCRIPTION

""

::= { ikeActionEntry 4 }

ikeProposalName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This row refers to an ikeProposalEntry in the ikeProposalTable."

```
::= { ikeActionEntry 5 }
```

ikeIdentityName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This row refers to an ikeIdentityEntry in the ikeIdentityTable."

::= { ikeActionEntry 6 }

ikeActionLastChange OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-create

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 }  
  
 --  
 -- 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 12 }

ikeProposalEntry OBJECT-TYPE

SYNTAX IkeProposalEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"One IKE proposal entry."

INDEX { ikeProposalName }

::= { ikeProposalTable 1 }

IkeProposalEntry ::= SEQUENCE {

ikeLifetimeDerivedKeys Unsigned32,

ikeCipherAlgorithm INTEGER,

ikeCipherKeyLength Unsigned32,

ikeCipherKeyRounds Unsigned32,

ikeHashAlgorithm INTEGER,

ikePrfAlgorithm INTEGER,

ikeVendorId OCTET STRING,

ikeDhGroup IpsecGroupId,

ikeAuthenticationMethod INTEGER,

ikeMaxLifetimeSeconds Unsigned32,

ikeMaxLifetimeKB Unsigned32,

ikeProposalLastChanged TimeStamp,

ikeProposalStorageType StorageType

}

ikeLifetimeDerivedKeys OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ikeLifetimeDerivedKeys 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 }

ikeCipherAlgorithm OBJECT-TYPE

SYNTAX INTEGER { desCbc(1), ideaCbc(2), blowfishCbc(3),

rc5Rc16B64Cbc(4), tripleDesCbc(5),

castCbc(6) }

MAX-ACCESS read-create
STATUS current

Various Authors

[Page 44]

DESCRIPTION

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

::= { ikeProposalEntry 2 }

ikeCipherKeyLength 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 }

ikeCipherKeyRounds 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 }

ikeHashAlgorithm OBJECT-TYPE

SYNTAX INTEGER { md5(1), sha(2), tiger(3) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ikeProposalEntry 5 }

ikePrfAlgorithm OBJECT-TYPE

SYNTAX INTEGER { reserved(0) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

Note: currently no prf algortithms are defined."

::= { ikeProposalEntry 6 }

ikeVendorId 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 }

ikeDhGroup OBJECT-TYPE

SYNTAX IpsecGroupId

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ikeProposalEntry 8 }

ikeAuthenticationMethod 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 }

ikeMaxLifetimeSeconds OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ikeProposalEntry 10 }

ikeMaxLifetimeKB OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ikeMaxLifetimeKB specifies the maximum kilobyte lifetime to propose a security association remain valid."

::= { ikeProposalEntry 11 }

ikeProposalLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-create

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 }
```

```
ikeProposalStorageType OBJECT-TYPE
```

```
SYNTAX      StorageType
```

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

```
STATUS      current
```

```
DESCRIPTION
```

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

```
but
```

```
which columns are in fact modifiable is implementation
```

```
specific."
```

```
::= { ikeProposalEntry 13 }
```

```
ikeProposalRowStatus 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 13 }
```

```
ipsecActionEntry OBJECT-TYPE
```

```
SYNTAX      IpsecActionEntry
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
"The ipsecActionEntry lists the IPsec negotiation attributes."
```

```
INDEX      { ipsecActionName }  
::= { ipsecActionTable 1 }
```

```

IpsecActionEntry ::= SEQUENCE {
    ipsecActionName          SnmpAdminString,
    ipsecProposalName       SnmpAdminString,
    ipsecUsePfs              TruthValue,
    ipsecVendorId           OCTET STRING,
    ipsecGroupId            INTEGER,
    ipsecUseIkeGroup        TruthValue,
    ipsecGranularity        INTEGER,
    ipsecMode               INTEGER,
    ipsecDFHandleing        INTEGER,
    ipsecActionLastChange   TimeStamp,
    ipsecActionStorageType  StorageType
}

```

```

ipsecActionName OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "ipsecActionName is the name of the ipsecAction entry."
    ::= { ipsecActionEntry 1 }

```

```

ipsecProposalName OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The name of an ipsecProposal referred to by this
         ipsecActionEntry."
    ::= { 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      IpsecGroupId  
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 }

-- PROPERTIES MinLifetimeSeconds

-- MinLifetimeKilobytes

-- RefreshThresholdSeconds

-- RefreshThresholdKilobytes

-- IdleDurationSeconds

ipsecActionLastChange OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-create

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 }
```

```
--
```

```
-- IPsec proposal definition table
```

```
--
```

```
ipsecProposalTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF IpsecProposalEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"This table lists the IPsec proposals for SA negotiations.
An IPsecProposal contains transform lists that specify the
phase 2 negotiation proposals for transform parameters.
```

```
Rows
```

```
in this table are referred to by the ipsecProposalName
```

```
column
```

```
from the ipsecAction table."
```

```
::= { ipsecPolicyConfigObjects 14 }
```

```
ipsecProposalEntry OBJECT-TYPE
```

```
SYNTAX IpsecProposalEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"An entry containing the information on an IPsec proposal."
```

```
INDEX { ipsecProposalName }
```

```
::= { ipsecProposalTable 1 }
```

```
IpsecProposalEntry ::= SEQUENCE {
```

```
ipsecProposalName SnmpAdminString,
```

```
ipsecProposalSet INTEGER,
```

```
ipsecAhTransformSet SnmpAdminString,
```

```
ipsecEspTransformSet SnmpAdminString,
```

```
ipsecIpcompTransformSet SnmpAdminString,
```

```
ipsecLastChanged TimeStamp,
```

```
ipsecStorageType StorageType
```

```
}
```

```
ipsecProposalName OBJECT-TYPE
```

SYNTAX	SnmpAdminString
MAX-ACCESS	not-accessible
STATUS	current

DESCRIPTION

"This object contains the name of the entry. This row is referred to by the ipsecProposalName column from an ipsecActionEntry."
 ::= { ipsecProposalEntry 1 }

ipsecProposalSet OBJECT-TYPE

SYNTAX INTEGER { esp(1), espAndAh(2), ah(3), ipcomp(4),
 ipcompAndEsp(5), ipcompAndEspAndAh(6) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "An ipsecProposal informs a system which protocol or combination of protocols to build an SA (bundle) with. Only a certain few combinations are sensible."
 ::= { ipsecProposalEntry 2 }

ipsecAhTransformSet OBJECT-TYPE

SYNTAX SnmpAdminString
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "If and only if the AH protocol is called for by the ipsecProposalSet, then this row will refer to a (list of) AhTransformEntry(s). Otherwise, any value in this column is ignored."
 ::= { ipsecProposalEntry 3 }

ipsecEspTransformSet OBJECT-TYPE

SYNTAX SnmpAdminString
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "If and only if the ESP protocol is called for by the ipsecProposalSet, then this row will refer to a (list of) ESPTransformEntry(s). Otherwise, any value in this column is ignored."
 ::= { ipsecProposalEntry 4 }

ipsecIpcompTransformSet OBJECT-TYPE

SYNTAX SnmpAdminString
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "If and only if the IPCOMP protocol is called for by the ipsecProposalSet, then this row will refer to a (list of) IPCOMPTransformEntry(s). Otherwise, any value in this column

is

```
    ignored."  
 ::= { ipsecProposalEntry 5 }
```

```
ipsecLastChanged OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-create
    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 6 }

ipsecStorageType 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 7 }

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.

        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 8 }

--
-- 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 15 }

ahTransformEntry OBJECT-TYPE

SYNTAX AhTransformEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

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

INDEX { ahTransformName }

::= { ahTransformTable 1 }

AhTransformEntry ::= SEQUENCE {

ahTransformName	SnmpAdminString,
ahTransformPriority	Unsigned32,
ahTransformId	INTEGER,
ahAntiReplay	Unsigned32,
ahTransformLastChanged	TimeStamp,
ahTransformStorageType	StorageType

}

ahTransformName OBJECT-TYPE

SYNTAX SnmpAdminString

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. If a list of ahTransformEntries all have the same name, then they are priority sorted by ahTransformPriority. "

::= { ahTransformEntry 1 }

ahTransformPriority OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ahTransformPriority indicates the preferability of this transform proposal. For the set of ahTransformEntries which have the same ahTransformName, the ahTransformPriority must

be

unique for each member on the list, must start at 1 and monotonically increase to the last member of the list. Lower

numbers indicate higher preferability."
 ::= { ahTransformEntry 2 }

ahTransformId OBJECT-TYPE

SYNTAX INTEGER { ahMd5(2), ahSha(3), ahDes(4) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies specifies the transform ID of the AH algorithm to propose during a Phase 2 SA negotiation."

::= { ahTransformEntry 3 }

ahAntiReplay OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ahAntiReplay indicates wether or not anti replay service is to be provided by this SA."

::= { ahTransformEntry 4 }

ahTransformLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-create

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 5 }

ahTransformStorageType 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 6 }

ahTransformRowStatus 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 7 }

--
-- 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 16 }

espTransformEntry OBJECT-TYPE
    SYNTAX      EspTransformEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This entry contains the attributes of one ESP transform."
    INDEX       { espTransformName }
    ::= { espTransformTable 1 }

EspTransformEntry ::= SEQUENCE {
    espTransformName          SnmpAdminString,
    espTransformPriority      Unsigned32,
    espCipherTransformId     INTEGER,
    espCipherKeyLength       Unsigned32,
    espCipherKeyRounds       Unsigned32,
    espIntegrityTransformId  INTEGER,
    espAntiReplay            Unsigned32,
    espTransformLastChange   TimeStamp,
    espTransformStorageType  StorageType
}

espTransformName OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  not-accessible
    STATUS      current

```

DESCRIPTION

"The name of this particular espTransformEntry. This row will

be referred to by an ipsecProposalEntry. If a list of espTransformEntries all have the same name, then they are priority sorted by espTransformPriority. "

```
::= { espTransformEntry 1 }
```

espTransformPriority OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"espTransformPriority indicates the preferability of this transform proposal. For the set of espTransformEntries which have the same espTransformName, the espTransformPriority must be unique for each member on the list, must start at 1 and monotonically increase to the last member of the list. Lower numbers indicate higher preferability."

```
::= { espTransformEntry 2 }
```

espCipherTransformId OBJECT-TYPE

```
SYNTAX INTEGER { espDesIv64(1), espDes(2), esp3Des(3),  
espRc5(4),  
espIdea(5), espCast(6), espBlowfish(7),  
esp3Idea(8), espDesIv32(9), espRc4(10),  
espNull(11) }
```

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

```
::= { espTransformEntry 3 }
```

espCipherKeyLength OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This mib object specifies, in bits, the key length for the ESP encryption algorithm."

```
::= { espTransformEntry 4 }
```

espCipherKeyRounds OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This mib object specifies the number of key rounds for

the ESP encryption algorithm."

Various Authors

[Page 57]

```
::= { espTransformEntry 5 }
```

```
espIntegrityTransformId OBJECT-TYPE
```

```
SYNTAX      INTEGER { hmacMd5(1), hmacSha(2), desMac(3), kpdk(4) }
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
    "This mib object specifies the transform ID of the ESP
```

```
integrity
```

```
    algorithm."
```

```
::= { espTransformEntry 6 }
```

```
espAntiReplay OBJECT-TYPE
```

```
SYNTAX      TruthValue
```

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

```
STATUS      current
```

```
DESCRIPTION
```

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

```
::= { espTransformEntry 7 }
```

```
espTransformLastChange OBJECT-TYPE
```

```
SYNTAX      TimeStamp
```

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

```
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 8 }
```

```
espTransformStorageType 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."
```

```
::= { espTransformEntry 9 }
```

```
espTransformRowStatus 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 10 }
```

```
--
-- 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 17 }
```

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,

ipcompTransformPriority Unsigned32,

ipcompAlgorithm INTEGER,

ipcompDictionarySize Unsigned32,

ipcompPrivateAlgorithm Unsigned32,

ipcompTransformLastChange TimeStamp,

ipcompTransformStorageType StorageType

}

ipcompTransformName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The name of this particular ipcompTransformEntry. This row will be referred to by an ipsecProposalEntry. If a list of ipcompTransformEntries all have the same name, then they are priority sorted by ipcompTransformPriority. "

::= { ipcompTransformEntry 1 }

ipcompTransformPriority OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipcompTransformPriority indicates the preferability of this transform proposal. For the set of ipcompTransformEntries which have the same ipcompTransformName, the ipcompTransformPriority must be unique for each member on the list, must start at 1 and monotonically increase to the last member of the list. Lower numbers indicate higher preferability."

::= { ipcompTransformEntry 2 }

ipcompAlgorithm OBJECT-TYPE

SYNTAX INTEGER { ipcompOui(1), ipcompDeflate(2), ipcompLzs(3)

}

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipcompAlgorithm specifies the transform ID of the IP compression algorithm."

::= { ipcompTransformEntry 3 }

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 4 }

ipcompPrivateAlgorithm OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current
DESCRIPTION

Various Authors

[Page 60]

"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 5 }

ipcompTransformLastChange OBJECT-TYPE

SYNTAX TimeStamp
MAX-ACCESS read-create
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 6 }

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 7 }

ipcompTransformRowStatus OBJECT-TYPE

SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the conceptual status of this row.

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

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 8 }

```
--  
-- IKE endpoint definition table  
--
```

Various Authors

[Page 61]

ikeIdentityTable OBJECT-TYPE

SYNTAX SEQUENCE OF IkeIdentityEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"IkeIdentity is used to represent the identities that may be used for an IPProtocolEndpoint (or collection of IPProtocolEndpoints) to identify itself in IKE phase 1 negotiations. The column .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 18 }
```

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 {

ikeIdentityName SnmpAdminString,

ikeIdentityType INTEGER,

ikeIdentityIdString OCTET STRING,

ikeIdentityIsOriginator INTEGER,

ikeIdentityLastChange TimeStamp,

ikeIdentityStorageType StorageType

}

ikeIdentityName OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"An administrative name for this row entry."

```
::= { ikeIdentityEntry 1 }
```

ikeIdentityType OBJECT-TYPE

SYNTAX INTEGER { ipv4Addr(1), fqdn(2), userAtFqdn(3),

ipV6AddrSubnet(6),
derAsn1Dn(9),
ipV4AddrSubnet(4), ipV6Addr(5),
ipV4AddrRange(7), ipV6AddrRange(8),

Various Authors

[Page 62]

```

        derAsn1Gn(10), keyId(11) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
    "The IdentityType specifies the type of IKE Identity."
 ::= { ikeIdentityEntry 2 }

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 3 }

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 4 }

ikeIdentityLastChange OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-create
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 5 }

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 6 }
```

```
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 7 }
```

```
END
```

6. Security Considerations

6.1 Introduction

This document defines an SNMP MIB used to configure IPsec. 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 show 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

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

8. Intellectual Property

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

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary

rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

9. 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.

