

IPSP Working Group
Internet Draft
[draft-ietf-ipsec-conf-mib-06.txt](#)

M. Baer
Network Associates Inc
R. Charlet
W. Hardaker
Network Associates Inc
R. Story
Revelstone Software
C. Wang
Smartpipes Inc
March 2003

IPsec Policy Configuration MIB module
draft-ietf-ipsec-conf-mib-06.txt

Status of this Memo

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

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

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

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

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This document defines a Management Information Base (MIB) module for managing the Internet Security Protocol (IPsec) and Internet Key Exchange (IKE) protocols and associated policies. Some of the policy-based packet filtering and the corresponding execution of actions is of a more general nature than for IPsec configuration only. This MIB module is designed with future extensibility in mind. It is thus possible to externally add other packet filters

and actions to the policy-based packet filtering system defined in this document.

Table of Contents

1.	Introduction	3
2.	The Internet-Standard Management Framework	3
3.	Relationship to the DMTF Policy Model	3
4.	MIB Module Overview	5
5.	Definitions	5
	ipspEndpointToGroupTable	9
	ipspGroupContentsTable	12
	ipspRuleDefinitionTable	15
	ipspCompoundFilterTable	18
	ipspSubfiltersTable	21
	ipspIpHeaderFilterTable	24
	ipspIpOffsetFilterTable	31
	ipspTimeFilterTable	35
	ipspIpsoHeaderFilterTable	39
	ipspCredentialFilterTable	41
	ipspPeerIdentityFilterTable	44
	ipspCompoundActionTable	46
	ipspSubactionsTable	48
	ipspSaPreconfiguredActionTable	52
	ipspSaNegotiationParametersTable	58
	ipspIkeActionTable	61
	ipspIkeActionProposalsTable	65
	ipspIkeProposalTable	67
	ipspIpsecActionTable	71
	ipspIpsecProposalsTable	75
	ipspIpsecTransformsTable	77
	ipspAhTransformTable	80
	ipspEspTransformTable	82
	ipspIpcompTransformTable	86
	ipspIkeIdentityTable	89
	ipspPeerIdentityTable	90
	ipspAutostartIkeTable	94
	ipspIpsecCredMngServiceTable	97
	ipspCredMngCRLTable	99
	ipspRevokedCertificateTable	102
	ipspCredentialTable	104
	ipspCredentialSegmentTable	107
6.	References	139

6.1.	Normative References	139
6.2.	Informative References	140
7.	Intellectual Property	140
8.	Security Considerations	140
8.1.	Introduction	140

8.2.	Protecting against in-authentic access	141
8.3.	Protecting against involuntary disclosure	142
8.4.	Bootstrapping your configuration	142
9.	Acknowledgments	142
10.	Authors' Addresses	143
11.	Full Copyright Statement	143

[1.](#) Introduction

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

[2.](#) The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to [section 7 of RFC 3410](#) [[RFC3410](#)]

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIV2, which is described in STD 58, [RFC 2578](#) [[RFC2578](#)], STD 58, [RFC 2579](#) [[RFC2579](#)] and STD 58, [RFC 2580](#) [[RFC2580](#)].

[3.](#) Relationship to the DMTF Policy Model

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

The high-level areas where this MIB module diverges from the IPCP model are:

- o Policies, Groups, Conditions, and some levels of Action are

Various Authors

[Page 3]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

generically named. That is we dropped prefixes like "SA", or "ipsec". This is because we feel that packet classification and matching of conditions to actions is more general than IPsec and could possibly be reused by other packet transforming actions which need to conditionally act on packets matching filters.

- o Filters are implemented in a more generic and scalable manner, rather than enforcing the condition/filtering pairing and their restrictions upon the user. The MIB module offers a compound filter object to provide for greater flexibility when creating complex filters.

[4.](#) MIB Module Overview

The MIB module is modularized into several different parts: rules, filters, and actions. The rules section connects endpoints and groups of rules together. This is partially made up of the `ipspEndpointToGroupTable`, `ipspGroupContentsTable`, and the `ipspRuleDefinitionTable`. Each row of the `ipspRuleDefinitionTable` connects a filter(s) with an action(s). It is structured to allow for reuse through the future creation of extension tables that provide additional filters and/or actions.

The filter section of the MIB module is composed of all the different types of filters in the Policy Model. It is partially made up of the `trueFilter`, `ipspCompoundFilterTable`, `ipspIpHeaderFilterTable`, `ipspIpOffsetFilterTable`, `ipspTimeFilterTable`, `ipspIpsoHeaderFilterTable`, `ipspCredentialFilterTable`, and the `ipspPeerIdentityFilterTable`.

The action section of the MIB module contains different action types from the Policy Model. It is also separated into Firewall actions (accept, drop, log, ...), IKE actions, and IPsec actions. It is partially made up of the `ipspStaticActions`, `ipspCompoundActionTable`,

ipspSaPreconfiguredActionTable, ipspIkeActionTable,
ipspIkeActionProposalsTable, ipspIkeIdentityTable,
ipspPeerIdentityTable, ipspIpsecActionTable,
ipspIpsecProposalsTable, ipspIpsecTransformsTable,
ipspAhTransformTable, and the ipspEspTransformTable.

5. Definitions

IPSEC-POLICY-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, Integer32,
Unsigned32, mib-2, experimental FROM SNMPv2-SMI

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

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

SnmpAdminString FROM SNMP-FRAMEWORK-MIB

Various Authors

[Page 5]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

InetAddressType, InetAddress, InetPortNumber
FROM INET-ADDRESS-MIB

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

--

-- module identity

--

ipspMIB MODULE-IDENTITY

LAST-UPDATED "200212100000Z" -- 12 December 2002

ORGANIZATION "IETF IP Security Policy Working Group"

CONTACT-INFO "Michael Baer

Network Associates, Inc.
3965 Freedom Circle, Suite 500
Santa Clara, CA 95054
Phone: +1 530 902 3131
Email: mike_baer@nai.com

Ricky Charlet
Email: rcharlet@alumni.calpoly.edu

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

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

Cliff Wang
SmartPipes Inc.
Suite 300, 565 Metro Place South
Dublin, OH 43017

Various Authors

[Page 6]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

Phone: +1 614 923 6241
E-Mail: CWang@smartpipes.com"

DESCRIPTION

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

Copyright (C) The Internet Society (2003). This version of this MIB module is part of RFC XXXX, see the RFC itself for full legal notices."

-- Revision History

REVISION "200301070000Z" -- 7 January 2003
DESCRIPTION "Initial version, published as RFC xxxx."
-- RFC-editor assigns xxxx

-- XXX: To be assigned by IANA
::= { mib-2 XXX }

--
-- groups of related objects
--

ipspConfigObjects OBJECT IDENTIFIER
::= { ipspMIB 1 }
ipspNotificationObjects OBJECT IDENTIFIER
::= { ipspMIB 2 }
ipspConformanceObjects OBJECT IDENTIFIER
::= { ipspMIB 3 }

--
-- Textual Conventions
--

IpspBooleanOperator ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION
"The IpspBooleanOperator 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(1), and(2) }

IpspAdminStatus ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION
"The IpspAdminStatus is used to specify the administrative
status of an object. Objects which are disabled must not
be used by the packet processing engine."

Various Authors

[Page 7]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

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

IpspSADirection ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"The IpspSADirection operator is used to specify whether or not a row should apply to outgoing or incoming SAs."

SYNTAX INTEGER { outgoing(1), incoming(2) }

IpspIPPacketLogging ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"IpspIPPacketLogging specifies whether or not an audit message should be logged when a packet is passed through an SA. A value of '-1' indicates no logging. A value of '0' or greater indicates that logging should be done and how many bytes of the beginning of the packet to place in the log. Values greater than the size of the packet being processed indicate that the entire packet should be sent.

Examples:

'-1' no logging

'0' log but do not include any of the packet in the log

'20' log and include the first 20 bytes of the packet in the log."

SYNTAX Integer32 (-1..65536)

IpspIdentityFilter ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"IpspIdentityFilter contains a string encoded Identity Type value to be used in comparisons against an IKE Identity payload. Wherever this TC is used, there should be an accompanying column which uses the IpsecDoiIdentType TC to specify the type of data in this object.

See the IpsecDoiIdentType TC for the supported identity types available. Note that the IpsecDoiIdentType TC specifies how to encode binary values, while this object will contain human readable string versions."

SYNTAX OCTET STRING (SIZE(1..256))

IpspCredentialType ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"IpspCredentialType identifies the type of credential contained in a corresponding IpspIdentityFilter object."

SYNTAX INTEGER { reserved(0),

```
        unknown(1),
        sharedSecret(2),
        x509(3),
        kerberos(4) }
```

```
--
```

```
-- Policy group definitions
```

```
--
```

```
ipspLocalConfigObjects OBJECT IDENTIFIER
```

```
 ::= { ipspConfigObjects 1 }
```

```
ipspSystemPolicyGroupName OBJECT-TYPE
```

```
 SYNTAX      SnmpAdminString (SIZE(0..32))
```

```
 MAX-ACCESS  read-write
```

```
 STATUS      current
```

```
 DESCRIPTION
```

```
 "This object indicates the policy group containing the global
 system policy that is to be applied when a given endpoint
 does not contain a policy definition. Its value can be used
 as an index into the ipspGroupContentsTable to retrieve a
 list of policies. A zero length string indicates no system
 wide policy exists and the default policy of 'accept' should
 be executed until one is imposed by either this object or by
 the endpoint processing a given packet."
```

```
 ::= { ipspLocalConfigObjects 1 }
```

```
ipspEndpointToGroupTable OBJECT-TYPE
```

```
 SYNTAX      SEQUENCE OF IspEndpointToGroupEntry
```

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

```
 STATUS      current
```

```
 DESCRIPTION
```

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

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

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

```
 ::= { ipspConfigObjects 2 }
```

ipspEndpointToGroupEntry OBJECT-TYPE

Various Authors

[Page 9]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

```
SYNTAX      IspspEndpointToGroupEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "A mapping assigning a policy group to an endpoint."
INDEX       { ipspEndGroupIdentType, ipspEndGroupAddress }
 ::= { ipspEndpointToGroupTable 1 }
```

```
IspspEndpointToGroupEntry ::= SEQUENCE {
    ipspEndGroupIdentType      InetAddressType,
    ipspEndGroupAddress        InetAddress,
    ipspEndGroupName          SnmpAdminString,
    ipspEndGroupLastChanged    TimeStamp,
    ipspEndGroupStorageType    StorageType,
    ipspEndGroupRowStatus     RowStatus
}
```

ipspEndGroupIdentType OBJECT-TYPE

```
SYNTAX      InetAddressType
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "The Internet Protocol version of the address associated with
    a given endpoint.  All addresses are represented as an array
    of octets in network byte order.  When combined with the
    ipspEndGroupAddress these objects can be used to uniquely
    identify an endpoint that a set of policy groups should be
    applied to.  Devices supporting IPv4 MUST support the ipv4
    value, and devices supporting IPv6 MUST support the ipv6
    value.

    Values of unknown, ipv4z, ipv6z and dns are not legal values
    for this object."
 ::= { ipspEndpointToGroupEntry 1 }
```

ipspEndGroupAddress OBJECT-TYPE

```
SYNTAX      InetAddress (SIZE (4|16))
MAX-ACCESS  not-accessible
STATUS      current
```

DESCRIPTION

"The address of a given endpoint, the format of which is specified by the ipspEndGroupIdentType object."
 ::= { ipspEndpointToGroupEntry 2 }

ipspEndGroupName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS read-create

Various Authors

[Page 10]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

STATUS current

DESCRIPTION

"The policy group name to apply to this endpoint. The value of the ipspEndGroupName object should then be used as an index into the ipspGroupContentsTable to come up with a list of rules that MUST be applied to this endpoint."
 ::= { ipspEndpointToGroupEntry 3 }

ipspEndGroupLastChanged OBJECT-TYPE

SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."
 ::= { ipspEndpointToGroupEntry 4 }

ipspEndGroupStorageType 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."
 DEFVAL { nonVolatile }
 ::= { ipspEndpointToGroupEntry 5 }

ipspEndGroupRowStatus OBJECT-TYPE

SYNTAX RowStatus
MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

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

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

::= { ipspEndpointToGroupEntry 6 }

--

-- policy group definition table

--

Various Authors

[Page 11]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

ipspGroupContentsTable OBJECT-TYPE

SYNTAX SEQUENCE OF IspspGroupContentsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

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

::= { ipspConfigObjects 3 }

ipspGroupContentsEntry OBJECT-TYPE

SYNTAX IspspGroupContentsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

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

INDEX { ipspGroupContName, ipspGroupContPriority }

```
::= { ipspGroupContentsTable 1 }
```

```
IpspGroupContentsEntry ::= SEQUENCE {  
    ipspGroupContName          SnmpAdminString,  
    ipspGroupContPriority      Integer32,  
    ipspGroupContFilter       VariablePointer,  
    ipspGroupContComponentType INTEGER,  
    ipspGroupContComponentName SnmpAdminString,  
    ipspGroupContLastChanged  TimeStamp,  
    ipspGroupContStorageType  StorageType,  
    ipspGroupContRowStatus    RowStatus  
}
```

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

```
ipspGroupContPriority OBJECT-TYPE  
    SYNTAX      Integer32 (0..65536)
```

Various Authors

[Page 12]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

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

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

evaluates to false, the rule or subgroup will be skipped and the next rule or subgroup will be evaluated instead.

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

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

```
    ipspIpHeaderFilterTable
    ipspIpOffsetFilterTable
    ipspTimeFilterTable
    ipspCompoundFilterTable
    ipspTrueFilter
```

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

```
DEFVAL { ipspTrueFilterInstance }
 ::= { ipspGroupContentsEntry 3 }
```

```
ipspGroupContComponentType OBJECT-TYPE
    SYNTAX      INTEGER { reserved(0), group(1), rule(2) }
    MAX-ACCESS  read-create
```

Various Authors

[Page 13]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

```
STATUS      current
```

```
DESCRIPTION
```

```
    "Indicates whether the ipspGroupContComponentName object is
     the name of another group defined within the
     ipspGroupContentsTable or is the name of a rule defined
     within the ipspRuleDefinitionTable."
```

```
DEFVAL { rule }
```

```
 ::= { ipspGroupContentsEntry 4 }
```

```
ipspGroupContComponentName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
```

MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The name of the policy rule or subgroup contained within this group, as indicated by the ipspGroupContComponentType object."
 ::= { ipspGroupContentsEntry 5 }

ipspGroupContLastChanged OBJECT-TYPE
SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."
 ::= { ipspGroupContentsEntry 6 }

ipspGroupContStorageType 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."
DEFVAL { nonVolatile }
 ::= { ipspGroupContentsEntry 7 }

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

The value of this object has no effect on whether other

objects in this conceptual row can be modified.

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


```

 ::= { ipspGroupContentsEntry 8 }

--
-- policy definition table
--

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

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

IspRuleDefinitionEntry ::= SEQUENCE {
    ipspRuleDefName          SnmpAdminString,
    ipspRuleDefDescription  SnmpAdminString,
    ipspRuleDefFilter        VariablePointer,
    ipspRuleDefFilterNegated TruthValue,
    ipspRuleDefAction        VariablePointer,
    ipspRuleDefAdminStatus   IspAdminStatus,
    ipspRuleDefLastChanged   TimeStamp,
    ipspRuleDefStorageType   StorageType,
    ipspRuleDefRowStatus     RowStatus
}

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

```

rule referred to by the ipspGroupContComponentName object."
 ::= { ipspRuleDefinitionEntry 1 }

ipspRuleDefDescription OBJECT-TYPE

SYNTAX SnmpAdminString

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

DEFVAL { "" }

::= { ipspRuleDefinitionEntry 2 }

ipspRuleDefFilter OBJECT-TYPE

SYNTAX VariablePointer

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

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

ipspIpHeaderFilterTable
ipspIpOffsetFilterTable
ipspTimeFilterTable
ipspCompoundFilterTable
ipspTrueFilter

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

::= { ipspRuleDefinitionEntry 3 }

ipspRuleDefFilterNegated OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-create

STATUS current

DESCRIPTION

Various Authors

[Page 16]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

"ipspRuleDefFilterNegated specifies whether the filter referenced by the ipspRuleDefFilter object should be negated or not."

DEFVAL { false }

::= { ipspRuleDefinitionEntry 4 }

ipspRuleDefAction OBJECT-TYPE

SYNTAX VariablePointer

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

 ipspCompoundActionTable
 ipspSaPreconfiguredActionTable
 ipspIkeActionTable
 ipspIpsecActionTable

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

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

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

::= { ipspRuleDefinitionEntry 5 }

ipspRuleDefAdminStatus OBJECT-TYPE

SYNTAX IspAdminStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Indicates whether the current rule definition should be considered active. If enabled, it should be evaluated when processing packets. If disabled, packets should continue to

be processed by the rest of the rules defined in the ipspGroupContentsTable as if this rule's filters had effectively failed."

DEFVAL { enabled }
 ::= { ipspRuleDefinitionEntry 6 }

ipspRuleDefLastChanged OBJECT-TYPE

SYNTAX TimeStamp

Various Authors

[Page 17]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

::= { ipspRuleDefinitionEntry 7 }

ipspRuleDefStorageType 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."

DEFVAL { nonVolatile }

::= { ipspRuleDefinitionEntry 8 }

ipspRuleDefRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

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

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

```
::= { ipspRuleDefinitionEntry 9 }
```

```
--
```

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

```
--
```

```
ipspCompoundFilterTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF IpspCompoundFilterEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"A table defining a compound set of filters and their associated parameters. A row in this table can either be pointed to by a ipspRuleDefFilter object or by a ficSubFilter object."
```

```
Various Authors
```

```
[Page 18]
```

```
Internet Draft IPsec Policy Configuration MIB module
```

```
Mar. 2003
```

```
::= { ipspConfigObjects 5 }
```

```
ipspCompoundFilterEntry OBJECT-TYPE
```

```
SYNTAX IpspCompoundFilterEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"An entry in the ipspCompoundFilterTable. A filter defined by this table is considered to have a TRUE return value if and only if:
```

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

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

```
INDEX { ipspCompFiltName }
```

```
::= { ipspCompoundFilterTable 1 }
```

```
IpspCompoundFilterEntry ::= SEQUENCE {
```

```
    ipspCompFiltName
```

```
    SnmpAdminString,
```

```

    ipspCompFiltDescription      SnmpAdminString,
    ipspCompFiltLogicType        IpspBooleanOperator,
    ipspCompFiltLastChanged      TimeStamp,
    ipspCompFiltStorageType      StorageType,
    ipspCompFiltRowStatus        RowStatus
}

```

```

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

```

```

ipspCompFiltDescription OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "A user definable string.  You may use this field for your

```

```

        administrative tracking purposes."
    DEFVAL { 'H' }
    ::= { ipspCompoundFilterEntry 2 }

```

```

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

```

```

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

```

DESCRIPTION

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

::= { ipspCompoundFilterEntry 4 }

ipspCompFiltStorageType 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."

DEFVAL { nonVolatile }

::= { ipspCompoundFilterEntry 5 }

ipspCompFiltRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

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

Once active, it may not have its value changed if any active rows in the ipspRuleDefinitionTable are currently pointing

at this row."

::= { ipspCompoundFilterEntry 6 }

--

-- Policy filters in a cf table

--

ipspSubfiltersTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpspSubfiltersEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This table defines a list of filters contained within a given compound filter set defined in the ipspCompoundFilterTable."
 ::= { ipspConfigObjects 6 }

ipspSubfiltersEntry OBJECT-TYPE
SYNTAX IpspSubfiltersEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"An entry into the list of filters for a given compound filter."
INDEX { ipspCompFiltName, ipspSubFiltPriority }
 ::= { ipspSubfiltersTable 1 }

IpspSubfiltersEntry ::= SEQUENCE {
 ipspSubFiltPriority Integer32,
 ipspSubFiltSubfilter VariablePointer,
 ipspSubFiltSubfilterIsNegated TruthValue,
 ipspSubFiltLastChanged TimeStamp,
 ipspSubFiltStorageType StorageType,
 ipspSubFiltRowStatus RowStatus
}

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

ipspSubFiltSubfilter OBJECT-TYPE

Various Authors

[Page 21]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

SYNTAX VariablePointer
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"The location of the contained filter. The value of this

column should be a VariablePointer which references the properties for the filter to be included in this compound filter.

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

```
    ipspIpHeaderFilterTable
    ipspIpOffsetFilterTable
    ipspTimeFilterTable
    ipspCompoundFilterTable
    ipspTrueFilter
```

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

```
::= { ipspSubfiltersEntry 2 }
```

ipspSubFiltSubfilterIsNegated OBJECT-TYPE

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

DESCRIPTION

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

```
DEFVAL { false }
```

```
::= { ipspSubfiltersEntry 3 }
```

ipspSubFiltLastChanged OBJECT-TYPE

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

DESCRIPTION

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

```
::= { ipspSubfiltersEntry 4 }
```

ipspSubFiltStorageType 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."

DEFVAL { nonVolatile }

::= { ipspSubfiltersEntry 5 }

ipspSubFiltRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

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

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

::= { ipspSubfiltersEntry 6 }

--

-- Static Filters

--

ipspStaticFilters OBJECT IDENTIFIER ::= { ipspConfigObjects 7 }

ipspTrueFilter OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This scalar indicates a (automatic) true result for a filter. I.e. this is a filter that is always true, useful for adding as a default filter for a default action or a set of actions."

::= { ipspStaticFilters 1 }

ipspTrueFilterInstance OBJECT IDENTIFIER ::= { ipspTrueFilter 0 }

ipspIkePhase1Filter OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-only

ipspIpHeadFiltSrcAddressBegin	InetAddress,
ipspIpHeadFiltSrcAddressEnd	InetAddress,
ipspIpHeadFiltDstAddressBegin	InetAddress,
ipspIpHeadFiltDstAddressEnd	InetAddress,
ipspIpHeadFiltSrcLowPort	InetPortNumber,
ipspIpHeadFiltSrcHighPort	InetPortNumber,

Various Authors

[Page 24]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

ipspIpHeadFiltDstLowPort	InetPortNumber,
ipspIpHeadFiltDstHighPort	InetPortNumber,
ipspIpHeadFiltProtocol	Integer32,
ipspIpHeadFiltIPv6FlowLabel	Integer32,
ipspIpHeadFiltLastChanged	TimeStamp,
ipspIpHeadFiltStorageType	StorageType,
ipspIpHeadFiltRowStatus	RowStatus

}

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

ipspIpHeadFiltType OBJECT-TYPE
 SYNTAX BITS { sourceAddress(0), destinationAddress(1),
 sourcePort(2), destinationPort(3),
 protocol(4), ipv6FlowLabel(5) }
 MAX-ACCESS read-create
 STATUS current
 DESCRIPTION
 "This defines the various tests that are used when evaluating
 a given filter. The results of each test are ANDed together
 to produce the result of the entire filter. When processing
 this filter, it is recommended for efficiency reasons that
 the filter halt processing the instant any of the specified
 tests fail.

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

The various tests definable in this table are as follows:

sourceAddress:

- Tests if the source address in the packet lies between the `ipspIpHeadFiltSrcAddressBegin` and `ipspIpHeadFiltSrcAddressEnd` objects.

Note that setting these two objects to the same address will limit the search to the exact match of a single address. The format and length of the address objects are defined by the `ipspIpHeadFiltIPVersion` column.

A row in this table containing a `ipspIpHeadFiltType` object with the `sourceAddress` object bit but without the `ipspIpHeadFiltIPVersion`, `ipspIpHeadFiltSrcAddressBegin` and `ipspIpHeadFiltSrcAddressEnd` objects set will cause the `ipspIpHeadFiltRowStatus` object to return the `notReady` state.

destinationAddress:

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

A row in this table containing a `ipspIpHeadFiltType` object with the `destinationAddress` object bit but without the `ipspIpHeadFiltIPVersion`, `ipspIpHeadFiltDstAddressBegin` and

`ipspIpHeadFiltDstAddressEnd` objects set will cause the `ipspIpHeadFiltRowStatus` object to return the `notReady` state.

sourcePort:

- Tests if the source port of IP packets using a protocol that uses port numbers (at this time, UDP or TCP) lies

between the `ipspIpHeadFiltSrcLowPort` and `ipspIpHeadFiltSrcHighPort` objects. Note that setting these two objects to the same address will limit the search to the exact match of a single port.

A row in this table containing a `ipspIpHeadFiltType` object with the `sourcePort` object bit but without the `ipspIpHeadFiltSrcLowPort`, and `ipspIpHeadFiltSrcHighPort` objects set will cause the `ipspIpHeadFiltRowStatus` object to return the `notReady` state.

`destinationPort`:

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

A row in this table containing a `ipspIpHeadFiltType`

object with the `sourcePort` object bit but without the `ipspIpHeadFiltDstLowPort`, and `ipspIpHeadFiltDstHighPort` objects set will cause the `ipspIpHeadFiltRowStatus` object to return the `notReady` state.

`protocol`:

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

A row in this table containing a `ipspIpHeadFiltType` object with the `protocol` object bit but without the `ipspIpHeadFiltProtocol` object set will cause the `ipspIpHeadFiltRowStatus` object to return the `notReady` state.

`ipv6FlowLabel`:

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

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

::= { ipspIpHeaderFilterEntry 2 }

ipspIpHeadFiltIPVersion OBJECT-TYPE

SYNTAX InetAddressType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The Internet Protocol version the addresses are to match against. The value of this property determines the size and format of the ipspIpHeadFiltSrcAddressBegin, ipspIpHeadFiltSrcAddressEnd, ipspIpHeadFiltDstAddressBegin, and ipspIpHeadFiltDstAddressEnd objects.

Values of unknown, ipv4z, ipv6z and dns are not legal values for this object."

DEFVAL { ipv6 }

::= { ipspIpHeaderFilterEntry 3 }

ipspIpHeadFiltSrcAddressBegin OBJECT-TYPE

SYNTAX InetAddress

MAX-ACCESS read-create

Various Authors

[Page 27]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

STATUS current

DESCRIPTION

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

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

::= { ipspIpHeaderFilterEntry 4 }

ipspIpHeadFiltSrcAddressEnd OBJECT-TYPE

SYNTAX InetAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

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

::= { ipspIpHeaderFilterEntry 5 }

ipspIpHeadFiltDstAddressBegin OBJECT-TYPE

SYNTAX InetAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

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

::= { ipspIpHeaderFilterEntry 6 }

ipspIpHeadFiltDstAddressEnd OBJECT-TYPE

SYNTAX InetAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

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

::= { ipspIpHeaderFilterEntry 7 }

ipspIpHeadFiltSrcLowPort OBJECT-TYPE

SYNTAX InetPortNumber

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

This object is only used if sourcePort is set in ipspIpHeadFiltType.

The value of 0 for this object is illegal."

::= { ipspIpHeaderFilterEntry 8 }

ipspIpHeadFiltSrcHighPort OBJECT-TYPE

SYNTAX InetPortNumber

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

This object is only used if sourcePort is set in ipspIpHeadFiltType.

The value of 0 for this object is illegal."

::= { ipspIpHeaderFilterEntry 9 }

ipspIpHeadFiltDstLowPort OBJECT-TYPE

SYNTAX InetPortNumber

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

This object is only used if destinationPort is set in ipspIpHeadFiltType.

The value of 0 for this object is illegal."

::= { ipspIpHeaderFilterEntry 10 }

ipspIpHeadFiltDstHighPort OBJECT-TYPE

SYNTAX InetPortNumber

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

This object is only used if destinationPort is set in ipspIpHeadFiltType.

The value of 0 for this object is illegal."

::= { ipspIpHeaderFilterEntry 11 }

ipspIpHeadFiltProtocol OBJECT-TYPE

SYNTAX Integer32 (0..255)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

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

::= { ipspIpHeaderFilterEntry 12 }

ipspIpHeadFiltIPv6FlowLabel OBJECT-TYPE

SYNTAX Integer32 (0..1048575)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

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

::= { ipspIpHeaderFilterEntry 13 }

ipspIpHeadFiltLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

::= { ipspIpHeaderFilterEntry 14 }

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

ipspIpHeadFiltStorageType 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."

DEFVAL { nonVolatile }

::= { ipspIpHeaderFilterEntry 15 }

ipspIpHeadFiltRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

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

::= { ipspIpHeaderFilterEntry 16 }

--

-- Policy IP Offset filter definition table

--

ipspIpOffsetFilterTable OBJECT-TYPE

SYNTAX SEQUENCE OF IspIpOffsetFilterEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This table contains a list of filter definitions to be used within the ipspRuleDefinitionTable or the ipspSubfilterTable."

::= { ipspConfigObjects 9 }

ipspIpOffsetFilterEntry OBJECT-TYPE

SYNTAX IpspIpOffsetFilterEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "A definition of a particular filter."

Various Authors

[Page 31]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

INDEX { ipspIpOffFiltName }
 ::= { ipspIpOffsetFilterTable 1 }

IpspIpOffsetFilterEntry ::= SEQUENCE {
 ipspIpOffFiltName SnmpAdminString,
 ipspIpOffFiltOffset Integer32,
 ipspIpOffFiltType INTEGER,
 ipspIpOffFiltNumber Integer32,
 ipspIpOffFiltValue OCTET STRING,
 ipspIpOffFiltLastChanged TimeStamp,
 ipspIpOffFiltStorageType StorageType,
 ipspIpOffFiltRowStatus RowStatus
}

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

ipspIpOffFiltOffset OBJECT-TYPE
SYNTAX Integer32 (0..65536)
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "This is the byte offset from the front of the IP packet where
 the value or arithmetic comparison is done. A value of '0'
 indicates the first byte in the packet."
 ::= { ipspIpOffsetFilterEntry 2 }

ipspIpOffFiltType OBJECT-TYPE
SYNTAX INTEGER { valueMatch(1),
 valueNotMatch(2),
 arithmeticEqual(3),

```
    arithmeticNotEqual(4),
    arithmeticLess(5),
    arithmeticGreaterOrEqual(6),
    arithmeticGreater(7),
    arithmeticLessOrEqual(8) }
```

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This defines the various tests that are used when evaluating a given filter.

Once a row is 'active', this object's value may not be

Various Authors

[Page 32]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

changed unless the appropriate columns, `ipspIpOffFiltNumber` or `ipspIpOffFiltValue`, needed by the new value to be imposed on this object have been appropriately configured.

The various tests definable in this table are as follows:

`valueMatch`:

- Tests if the OCTET STRING, '`ipspIpOffFiltValue`', matches a value in the packet starting at the given offset in the packet and comparing the entire OCTET STRING of '`ipspIpOffFiltValue`'.

`valueNotMatch`:

- Tests if the OCTET STRING, '`ipspIpOffFiltValue`', does not match a value in the packet starting at the given offset in the packet and comparing to the entire OCTET STRING of '`ipspIpOffFiltValue`'.

`arithmeticEqual`:

- Tests if the Integer32, '`ipspIpOffFiltNumber`', is arithmetically equal ('=') to the 4 byte value starting at the given offset within the packet. The value in the packet is assumed to be in network byte order.

`arithmeticNotEqual`:

- Tests if the Integer32, '`ipspIpOffFiltNumber`', is arithmetically not equal ('!=') to the 4 byte value starting at the given offset within the packet. The value in the packet is assumed to be in network byte

order.

arithmeticLess:

- Tests if the Integer32, 'ipspIpOffFiltNumber', is arithmetically less than ('<') the 4 byte value starting at the given offset within the packet. The value in the packet is assumed to be in network byte order.

arithmeticGreaterOrEqual:

- Tests if the Integer32, 'ipspIpOffFiltNumber', is arithmetically greater than or equal to ('>=') the 4 byte value starting at the given offset within the packet. The value in the packet is assumed to be in network byte order.

arithmeticGreater:

- Tests if the Integer32, 'ipspIpOffFiltNumber', is arithmetically greater than ('>') the 4 byte value starting at the given offset within the packet. The

value in the packet is assumed to be in network byte order.

arithmeticLessOrEqual:

- Tests if the Integer32, 'ipspIpOffFiltNumber', is arithmetically less than or equal to ('<=') the 4 byte value starting at the given offset within the packet. The value in the packet is assumed to be in network byte order."

::= { ipspIpOffsetFilterEntry 3 }

ipspIpOffFiltNumber OBJECT-TYPE

SYNTAX Integer32 (0..65536)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipspIpOffFiltNumber is used for arithmetic matching of a packets at ipspIpOffFiltOffset. This object is only used if one of the arithmetic types is chosen in ipspIpOffFiltType."

```
::= { ipspIpOffsetFilterEntry 4 }
```

```
ipspIpOffFiltValue OBJECT-TYPE
```

```
SYNTAX OCTET STRING (SIZE(0..1024))
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"ipspIpOffFiltValue is used for match comparisons of a packet at  
ipspIpOffFiltOffset. This object is only used if one of the  
match types is chosen in ipspIpOffFiltType."
```

```
::= { ipspIpOffsetFilterEntry 5 }
```

```
ipspIpOffFiltLastChanged OBJECT-TYPE
```

```
SYNTAX TimeStamp
```

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

```
STATUS current
```

```
DESCRIPTION
```

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

```
::= { ipspIpOffsetFilterEntry 6 }
```

```
ipspIpOffFiltStorageType OBJECT-TYPE
```

```
SYNTAX StorageType
```

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

Various Authors

[Page 34]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

```
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."
```

```
DEFVAL { nonVolatile }
```

```
::= { ipspIpOffsetFilterEntry 7 }
```

```
ipspIpOffFiltRowStatus OBJECT-TYPE
```

```
SYNTAX RowStatus
```

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

```
STATUS current
```

```
DESCRIPTION
```

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

This object may not be set to active if the requirements of the ipspIpOffFiltType object are not met. In other words, if the associated value columns needed by a particular test have not been set, then attempting to change this row to an active state will result in an inconsistentValue error. See the ipspIpOffFiltType object description for further details."
 ::= { ipspIpOffsetFilterEntry 8 }

--
--
--

ipspTimeFilterTable OBJECT-TYPE

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

"Defines a table of filters which can be used to effectively enable or disable policies based on a valid time range."

::= { ipspConfigObjects 10 }

ipspTimeFilterEntry OBJECT-TYPE

SYNTAX IspTimeFilterEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

"A row describing a given time frame for which a policy may be filtered on to place the rule active or inactive."

INDEX { ipspTimeFiltName }
 ::= { ipspTimeFilterTable 1 }

IspTimeFilterEntry ::= SEQUENCE {

ipspTimeFiltName	SnmpAdminString,
ipspTimeFiltPeriodStart	DateAndTime,
ipspTimeFiltPeriodEnd	DateAndTime,
ipspTimeFiltMonthOfYearMask	BITS,
ipspTimeFiltDayOfMonthMask	OCTET STRING,
ipspTimeFiltDayOfWeekMask	BITS,
ipspTimeFiltTimeOfDayMaskStart	DateAndTime,
ipspTimeFiltTimeOfDayMaskEnd	DateAndTime,


```
    ipspTimeFiltLastChanged      TimeStamp,
    ipspTimeFiltStorageType     StorageType,
    ipspTimeFiltRowStatus       RowStatus
}
```

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

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

```
ipspTimeFiltPeriodEnd OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The ending time period for this filter. In addition to a
        normal DateAndTime string, this object may be set to the
        OCTET STRING value THISANDFUTURE which indicates that the
        filter is valid without an ending date and/or time."
    DEFVAL { '99991231235959092b0000'H }
    ::= { ipspTimeFilterEntry 3 }
```

```

SYNTAX      BITS { january(0), february(1), march(2), april(3),
                may(4), june(5), july(6), august(7),
                september(8), october(9), november(10),
                december(11) }
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "A bit mask which overlays the ipspTimeFiltPeriodStart to
    ipspTimeFiltPeriodEnd date range to further restrict the time
    period to a restricted set of months of the year."
DEFVAL { { january, february, march, april, may, june, july,
            august, september, october, november, december } }
::= { ipspTimeFilterEntry 4 }

```

ipspTimeFiltDayOfMonthMask OBJECT-TYPE

```

SYNTAX      OCTET STRING (SIZE(4))
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "Defines which days of the month this time period is valid
    for. It is a sequence of 32 BITS, where each BIT represents
    a corresponding day of the month starting from the left most
    bit being equal to the first day of the month. The last bit
    in the string MUST be zero."
DEFVAL { 'fffffffH' }
::= { ipspTimeFilterEntry 5 }

```

ipspTimeFiltDayOfWeekMask OBJECT-TYPE

```

SYNTAX      BITS { monday(0), tuesday(1), wednesday(2),
                thursday(3), friday(4), saturday(5),
                sunday(6) }
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "A bit mask which overlays the ipspTimeFiltPeriodStart to
    ipspTimeFiltPeriodEnd date range to further restrict the time
    period to a restricted set of days within a given week."
DEFVAL { { monday, tuesday, wednesday, thursday, friday,
            saturday, sunday } }
::= { ipspTimeFilterEntry 6 }

```

ipspTimeFiltTimeOfDayMaskStart OBJECT-TYPE

```

SYNTAX      DateAndTime
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION

```

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

DEFVAL { '000000000000000002b0000'H }

::= { ipspTimeFilterEntry 7 }

ipspTimeFiltTimeOfDayMaskEnd OBJECT-TYPE

SYNTAX DateAndTime

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

DEFVAL { '000000000000000002b0000'H }

::= { ipspTimeFilterEntry 8 }

ipspTimeFiltLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

::= { ipspTimeFilterEntry 9 }

ipspTimeFiltStorageType 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."

DEFVAL { nonVolatile }

::= { ipspTimeFilterEntry 10 }

ipspTimeFiltRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create
STATUS current

DESCRIPTION

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

--
-- IPSO protection authority filtering
--

ipspIpssoHeaderFilterTable OBJECT-TYPE

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

DESCRIPTION

"This table contains a list of IPSO header filter definitions to be used within the ipspRuleDefinitionTable or the ipspSubfilterTable. IPSO headers and their values are described in [RFC1108](#)."
 ::= { ipspConfigObjects 11 }

ipspIpssoHeaderFilterEntry OBJECT-TYPE

SYNTAX IpspIpssoHeaderFilterEntry
MAX-ACCESS not-accessible
STATUS current

DESCRIPTION

"A definition of a particular filter."
 INDEX { ipspIpssoHeadFiltName }
 ::= { ipspIpssoHeaderFilterTable 1 }

IpspIpssoHeaderFilterEntry ::= SEQUENCE {

ipspIpssoHeadFiltName	SnmAdminString,
ipspIpssoHeadFiltType	BITS,
ipspIpssoHeadFiltClassification	INTEGER,
ipspIpssoHeadFiltProtectionAuth	INTEGER,
ipspIpssoHeadFiltLastChanged	TimeStamp,
ipspIpssoHeadFiltStorageType	StorageType,
ipspIpssoHeadFiltRowStatus	RowStatus

}

ipspIpssoHeadFiltName OBJECT-TYPE

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

ipspIpsHeaderFilterType OBJECT-TYPE
SYNTAX BITS { classificationLevel(0),

Various Authors

[Page 39]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

protectionAuthority(1) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The IPSO header fields to match the value against."
 ::= { ipspIpsHeaderFilterEntry 2 }

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

 The values of these enumerations are defined by [RFC1108](#)."
 ::= { ipspIpsHeaderFilterEntry 3 }

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

 The values of these enumerations are defined by [RFC1108](#).
 Hence the reason the SMIV2 convention of not using 0 in enum

```
lists is violated here."
 ::= { ipspIpsoHeaderFilterEntry 4 }
```

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

```
ipspIpsoHeadFiltStorageType OBJECT-TYPE
    SYNTAX      StorageType
    MAX-ACCESS  read-create
```

Various Authors

[Page 40]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

```
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."
DEFVAL { nonVolatile }
 ::= { ipspIpsoHeaderFilterEntry 6 }
```

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

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

--

```
-- credential filter table
--
```

```
ipspCredentialFilterTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IspCredentialFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table defines filters which can be used to match
         credentials of IKE peers, where the credentials in question
         have been obtained from an IKE phase 1 exchange.  They may be
         X.509 certificates, Kerberos tickets, etc..."
    ::= { ipspConfigObjects 12 }
```

```
ipspCredentialFilterEntry OBJECT-TYPE
    SYNTAX      IspCredentialFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row defining a particular credential filter"
    INDEX      { ipspCredFiltName }
    ::= { ipspCredentialFilterTable 1 }
```

Various Authors

[Page 41]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

```
IspCredentialFilterEntry ::= SEQUENCE {
    ipspCredFiltName          SnmpAdminString,
    ipspCredFiltCredentialType IspCredentialType,
    ipspCredFiltMatchFieldName OCTET STRING,
    ipspCredFiltMatchFieldValue OCTET STRING,
    ipspCredFiltAcceptCredFrom OCTET STRING,
    ipspCredFiltLastChanged   TimeStamp,
    ipspCredFiltStorageType   StorageType,
    ipspCredFiltRowStatus     RowStatus
}
```

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

```
ipspCredFiltCredentialType OBJECT-TYPE
    SYNTAX      IspspCredentialType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The credential type that is expected for this filter to
        succeed."
    DEFVAL { x509 }
    ::= { ipspCredentialFilterEntry 2 }
```

```
ipspCredFiltMatchFieldName OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..256))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The piece of the credential to match against.  Examples:
        serialNumber, signatureAlgorithm, issuerName or subjectName.

        For credential types without fields (e.g. shared secrec),
        this field should be left empty, and the entire credential
        will be matched against the ipspCredFiltMatchFieldValue."
    ::= { ipspCredentialFilterEntry 3 }
```

```
ipspCredFiltMatchFieldValue OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(1..4096))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The value that the field indicated by the
```

```
        ipspCredFiltMatchFieldName must match against for the filter
        to be considered TRUE."
    ::= { ipspCredentialFilterEntry 4 }
```

```
ipspCredFiltAcceptCredFrom OBJECT-TYPE
    SYNTAX      OCTET STRING(SIZE(1..117))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This value is used to look up a row in the
        ipspIpsecCredMngServiceTable for the Certificate Authority (CA)
```


Information. This value is empty if there is no CA used for this filter."

::= { ipspCredentialFilterEntry 5 }

ipspCredFiltLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

::= { ipspCredentialFilterEntry 6 }

ipspCredFiltStorageType 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."

DEFVAL { nonVolatile }

::= { ipspCredentialFilterEntry 7 }

ipspCredFiltRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspCredentialFilterEntry 8 }

--

-- Peer Identity Filter Table

--

Various Authors

[Page 43]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

ipspPeerIdentityFilterTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpspPeerIdentityFilterEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

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

::= { ipspConfigObjects 13 }

ipspPeerIdentityFilterEntry OBJECT-TYPE

SYNTAX IpspPeerIdentityFilterEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A row defining a particular credential filter"

INDEX { ipspPeerIdFiltName }

::= { ipspPeerIdentityFilterTable 1 }

IpspPeerIdentityFilterEntry ::= SEQUENCE {

ipspPeerIdFiltName	SnmpAdminString,
ipspPeerIdFiltIdentityType	IpsecDoiIdentType,
ipspPeerIdFiltIdentityValue	IpspIdentityFilter,
ipspPeerIdFiltLastChanged	TimeStamp,
ipspPeerIdFiltStorageType	StorageType,
ipspPeerIdFiltRowStatus	RowStatus

}

ipspPeerIdFiltName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(1..32))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The administrative name of this filter."

::= { ipspPeerIdentityFilterEntry 1 }

ipspPeerIdFiltIdentityType OBJECT-TYPE

SYNTAX IpsecDoiIdentType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The type of identity field in the peer ID payload to match against."

::= { ipspPeerIdentityFilterEntry 2 }

ipspPeerIdFiltIdentityValue OBJECT-TYPE

SYNTAX IpspIdentityFilter

MAX-ACCESS read-create
STATUS current
DESCRIPTION

"The string representation of the value that the peer ID payload value must match against. Wildcard mechanisms MUST be supported such that:

- a ipspPeerIdFiltIdentityValue of '*@example.com' will match a userFqdn ID payload of 'JDOE@EXAMPLE.COM'
- a ipspPeerIdFiltIdentityValue of '*.example.com' will match a fqdn ID payload of 'WWW.EXAMPLE.COM'
- a ipspPeerIdFiltIdentityValue of:
 'cn=*,ou=engineering,o=company,c=us'
will match a DER DN ID payload of
 'cn=John Doe,ou=engineering,o=company,c=us'
- a ipspPeerIdFiltIdentityValue of '192.0.2.0/24' will match an IPv4 address ID payload of 192.0.2.10
- a ipspPeerIdFiltIdentityValue of '192.0.2.*' will also match an IPv4 address ID payload of 192.0.2.10.

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

::= { ipspPeerIdentityFilterEntry 3 }

ipspPeerIdFiltLastChanged OBJECT-TYPE

SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION

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

::= { ipspPeerIdentityFilterEntry 4 }

ipspPeerIdFiltStorageType 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."

DEFVAL { nonVolatile }

```
::= { ipspPeerIdentityFilterEntry 5 }
```

```
ipspPeerIdFiltRowStatus OBJECT-TYPE
```

```
SYNTAX RowStatus
```

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

```
STATUS current
```

```
DESCRIPTION
```

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

```
    This object can not be considered active unless the
```

```
    ipspPeerIdFiltIdentityType and ipspPeerIdFiltIdentityValue  
    column values are defined."
```

```
::= { ipspPeerIdentityFilterEntry 6 }
```

```
--
```

```
-- compound actions table
```

```
--
```

```
ipspCompoundActionTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF IpspCompoundActionEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
    "Table used to allow multiple actions to be associated with a  
    rule. It uses the ipspSubactionsTable to do this."
```

```
::= { ipspConfigObjects 14 }
```

```
ipspCompoundActionEntry OBJECT-TYPE
```

```
SYNTAX IpspCompoundActionEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
    "A row in the ipspCompoundActionTable."
```

```
INDEX { ipspCompActName }
```

```
::= { ipspCompoundActionTable 1 }
```

```
IpspCompoundActionEntry ::= SEQUENCE {
```

```
    ipspCompActName
```

```
    ipspCompActExecutionStrategy
```

```
    ipspCompActLastChanged
```

```
    ipspCompActStorageType
```

```
    ipspCompActRowStatus
```

```
    SnmpAdminString,
```

```
    INTEGER,
```

```
    TimeStamp,
```

```
    StorageType,
```

```
    RowStatus
```

```
}
```

ipspCompActName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"This is an administratively assigned name of this compound
action."

Various Authors

[Page 46]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

::= { ipspCompoundActionEntry 1 }

ipspCompActExecutionStrategy OBJECT-TYPE
SYNTAX INTEGER { reserved(0),
doAll(1),
doUntilSuccess(2),
doUntilFailure(3) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object indicates how the sub-actions are executed based
on the success of the actions as they finish executing.

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

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

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

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

ipspCompActStorageType OBJECT-TYPE
SYNTAX StorageType
MAX-ACCESS read-create
STATUS current
DESCRIPTION

Various Authors

[Page 47]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

"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."
DEFVAL { nonVolatile }
 ::= { ipspCompoundActionEntry 4 }

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

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

Once a row in the ipspCompoundActionTable has been made active,
this object may not be set to destroy without first
destroying all the contained rows listed in the
ipspSubactionsTable."
 ::= { ipspCompoundActionEntry 5 }

--
-- actions contained within a compound action
--

```

ipspSubactionsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IspSubactionsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table contains a list of the sub-actions within a given
        compound action.  Compound actions executing these actions
        MUST execute them in series based on the ipspSubActPriority
        value, with the lowest value executing first."
    ::= { ipspConfigObjects 15 }

```

```

ipspSubactionsEntry OBJECT-TYPE
    SYNTAX      IspSubactionsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row containing a reference to a given compound-action
        sub-action."
    INDEX      { ipspCompActName, ipspSubActPriority }
    ::= { ipspSubactionsTable 1 }

```

```

IspSubactionsEntry ::= SEQUENCE {
    ipspSubActPriority          Integer32,
    ipspSubActSubActionName    VariablePointer,
    aiipspCompActLastChanged   TimeStamp,
    aiipspCompActStorageType   StorageType,
    aiipspCompActRowStatus    RowStatus
}

```

```

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

```

ipspSubActSubActionName OBJECT-TYPE

SYNTAX VariablePointer

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

ipspCompoundActionTable - Allowing recursion
ipspSaPreconfiguredActionTable
ipspIkeActionTable
ipspIpsecActionTable

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

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

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

::= { ipspSubactionsEntry 2 }

aiipspCompActLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

Various Authors

[Page 49]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

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."

::= { ipspSubactionsEntry 3 }

aiipspCompActStorageType 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."
    DEFVAL { nonVolatile }
    ::= { ipspSubactionsEntry 4 }

aiipspCompActRowStatus 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."
    ::= { ipspSubactionsEntry 5 }

--
-- Static Actions
--

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

ipspStaticActions OBJECT IDENTIFIER ::= { ipspConfigObjects 16 }

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

```

```

    ::= { ipspStaticActions 1 }

```

```

ipspDropActionLog OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only

```

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

ipspAcceptAction OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This Scalar indicates that a packet should be accepted
(pass-through) WITHOUT action/packet logging. This object
returns a value of 1 for IPsec policy implementations that
support the accept static action."
 ::= { ipspStaticActions 3 }

ipspAcceptActionLog OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This scalar indicates that a packet should be accepted
(pass-through) WITH action/packet logging. This object
returns a value of 1 for IPsec policy implementations that
support the accept static action with logging."
 ::= { ipspStaticActions 4 }

ipspRejectIKEAction OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"This scalar indicates that a packet should be rejected
WITHOUT action/packet logging. This object returns a value
of 1 for IPsec policy implementations that support the reject
static action."
 ::= { ipspStaticActions 5 }

ipspRejectIKEActionLog OBJECT-TYPE
SYNTAX Integer32

```

MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    "This scalar indicates that a packet should be rejected
    WITH action/packet logging. This object returns a value of 1
    for IPsec policy implementations that support the reject
    static action with logging."
 ::= { ipspStaticActions 6 }

--
-- Preconfigured Action Table
--

ipspSaPreconfiguredActionTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IspSaPreconfiguredActionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table is a list of non-negotiated IPsec actions (SAs)
        that can be performed and contains or indicates the data
        necessary to create such an SA."
    ::= { ipspConfigObjects 17 }

ipspSaPreconfiguredActionEntry OBJECT-TYPE
    SYNTAX      IspSaPreconfiguredActionEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "One entry in the ipspSaPreconfiguredActionTable."
    INDEX       { ipspSaPreActActionName, ipspSaPreActSADirection }
    ::= { ipspSaPreconfiguredActionTable 1 }

IspSaPreconfiguredActionEntry ::= SEQUENCE {
    ipspSaPreActActionName          SnmpAdminString,
    ipspSaPreActSADirection        IspSADirection,
    ipspSaPreActActionDescription  SnmpAdminString,
    ipspSaPreActActionLifetimeSec  Unsigned32,
    ipspSaPreActActionLifetimeKB   Unsigned32,
    ipspSaPreActDoActionLogging    TruthValue,
    ipspSaPreActDoPacketLogging    IspIPPacketLogging,
    ipspSaPreActDFHandling         INTEGER,
    ipspSaPreActActionType         IspSecDoiEncapsulationMode,
    ipspSaPreActAHSPI              Integer32,
    ipspSaPreActAHTransformName    SnmpAdminString,
    ipspSaPreActAHSharedSecretName SnmpAdminString,
    ipspSaPreActESPSPID            Integer32,

```

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

```
    ipspSaPreActESPTransformName      SnmpAdminString,
    ipspSaPreActESPEncSecretName      SnmpAdminString,
    ipspSaPreActESPAuthSecretName     SnmpAdminString,
    ipspSaPreActIPCompSPI             Integer32,
    ipspSaPreActIPCompTransformName   SnmpAdminString,
    ipspSaPreActPeerGatewayIdName     SnmpAdminString,
    ipspSaPreActLastChanged           TimeStamp,
    ipspSaPreActStorageType           StorageType,
    ipspSaPreActRowStatus             RowStatus
}

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

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

ipspSaPreActActionDescription OBJECT-TYPE
    SYNTAX           SnmpAdminString
    MAX-ACCESS       read-create
    STATUS            current
    DESCRIPTION
        "An administratively assigned string which may be used
         to describe what the action does."
    DEFVAL { "" }
    ::= { ipspSaPreconfiguredActionEntry 3 }

ipspSaPreActActionLifetimeSec OBJECT-TYPE
    SYNTAX           Unsigned32
```

MAX-ACCESS read-create
STATUS current
DESCRIPTION

"ipspSaPreActActionLifetimeSec specifies how long in seconds the security association derived from this action should be used. The default lifetime is 8 hours.

Various Authors

[Page 53]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

Note: the actual lifetime of the preconfigured SA will be the lesser of the value of this object and of the value of the MaxLifetimeSecs property of the associated transform.

A value of 0 indicates no time limit on the lifetime of the SA."

DEFVAL { 28800 }
 ::= { ipspSaPreconfiguredActionEntry 4 }

ipspSaPreActActionLifetimeKB OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"ipspSaPreActActionLifetimeKB specifies how long the security association derived from this action should be used. After this value in KiloBytes has passed through the security association, it should no longer be used.

Note: the actual lifetime of the preconfigured SA will be the lesser of the value of this object and of the value of the MaxLifetimeKB property of the associated transform.

The default value, '0', indicates no kilobyte limit."

DEFVAL { 0 }
 ::= { ipspSaPreconfiguredActionEntry 5 }

ipspSaPreActDoActionLogging OBJECT-TYPE

SYNTAX TruthValue
MAX-ACCESS read-create
STATUS current
DESCRIPTION

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

DEFVAL { false }

```
::= { ipspSaPreconfiguredActionEntry 6 }
```

```
ipspSaPreActDoPacketLogging OBJECT-TYPE
```

```
SYNTAX      IpspIPPacketLogging
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
"ipspSaPreActDoPacketLogging specifies whether or not an audit message should be logged and if there is logging, how many bytes of the packet to place in the notification."
```

```
DEFVAL { -1 }
```

```
::= { ipspSaPreconfiguredActionEntry 7 }
```

Various Authors

[Page 54]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

```
ipspSaPreActDFHandling OBJECT-TYPE
```

```
SYNTAX      INTEGER {
```

```
    reserved(0),  -- reserved
```

```
    copy(1),      -- indicates copy the DF bit from the  
                  -- internal to external IP header.
```

```
    set(2),       -- set the DF bit in the external IP  
                  -- header to 1.
```

```
    clear(3)      -- clear the DF bit in the external IP  
                  -- header to 0.
```

```
}
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
"This object specifies how to process the DF bit in packets sent through the preconfigured SA. This object is not used for transport SAs."
```

```
DEFVAL { copy }
```

```
::= { ipspSaPreconfiguredActionEntry 8 }
```

```
ipspSaPreActActionType OBJECT-TYPE
```

```
SYNTAX      IpsecDoiEncapsulationMode
```

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

```
STATUS      current
```

```
DESCRIPTION
```

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

```
DEFVAL { tunnel }
```

```
::= { ipspSaPreconfiguredActionEntry 9 }
```

ipspSaPreActAHSPI OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspSaPreconfiguredActionEntry 10 }

ipspSaPreActAHTransformName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspSaPreconfiguredActionEntry 11 }

ipspSaPreActAHSharedSecretName OBJECT-TYPE

Various Authors

[Page 55]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

SYNTAX SnmpAdminString(SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object contains a name value to be used as an index into the ipspCredentialTable which holds the pertinent keying information for the AH SA."

::= { ipspSaPreconfiguredActionEntry 12 }

ipspSaPreActESPSPPI OBJECT-TYPE

SYNTAX Integer32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspSaPreconfiguredActionEntry 13 }

ipspSaPreActESPTransformName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspSaPreconfiguredActionEntry 14 }

ipspSaPreActESPEncSecretName OBJECT-TYPE

SYNTAX SnmpAdminString(SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object contains a name value to be used as an index into the ipspCredentialTable which holds the pertinent keying information for the encryption algorithm of the ESP SA."

::= { ipspSaPreconfiguredActionEntry 15 }

ipspSaPreActESPAuthSecretName OBJECT-TYPE

SYNTAX SnmpAdminString(SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object contains a name value to be used as an index into the ipspCredentialTable which holds the pertinent keying information for the authentication algorithm of the ESP SA."

::= { ipspSaPreconfiguredActionEntry 16 }

ipspSaPreActIPCompSPI OBJECT-TYPE

Various Authors

[Page 56]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

SYNTAX Integer32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspSaPreconfiguredActionEntry 17 }

ipspSaPreActIPCompTransformName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object is the name of the IPComp transform to use as an index into the IPCompTransformTable. A zero length value

indicates no transform of this type is used."
 ::= { ipspSaPreconfiguredActionEntry 18 }

ipspSaPreActPeerGatewayIdName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the peer id name of the peer gateway. This object can be used to look up the peer gateway address in the ipspPeerIdentityTable.

This object is only used when initiating a tunnel SA, and is not used for transport SAs. If ipspSaPreActActionType specifies tunnel mode and this object is empty, the peer gateway should be determined from the source or destination of the packet."

DEFVAL { "" }

::= { ipspSaPreconfiguredActionEntry 19 }

ipspSaPreActLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

::= { ipspSaPreconfiguredActionEntry 20 }

ipspSaPreActStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

Various Authors

[Page 57]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

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."

DEFVAL { nonVolatile }

::= { ipspSaPreconfiguredActionEntry 21 }

```

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

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

        If active, this object must remain active if it is referenced
        by a row in another table."
 ::= { ipspSaPreconfiguredActionEntry 22 }

--
-- ipspSaNegotiationParametersTable
--
--
--     PROPERTIES   MinLifetimeSeconds
--                 MinLifetimeKilobytes
--                 RefreshThresholdSeconds
--                 RefreshThresholdKilobytes
--                 IdleDurationSeconds

ipspSaNegotiationParametersTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IpspSaNegotiationParametersEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table contains reusable parameters that can be pointed
        to by the ipspIkeActionTable and ipspIpsecActionTable. These
        parameters are reusable since it is likely an administrator
        will want to make global policy changes to lifetime
        parameters that apply to multiple actions. This table allows
        multiple rows in the other actions tables to reuse global
        lifetime parameters in this table by repeatedly pointing to a
        row contained within this table."
 ::= { ipspConfigObjects 18 }

ipspSaNegotiationParametersEntry OBJECT-TYPE

```

SYNTAX IpspSaNegotiationParametersEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "Contains the attributes of one row in the
 ipspSaNegotiationParametersTable."
INDEX { ipspSaNegParamName }
::= { ipspSaNegotiationParametersTable 1 }

IpspSaNegotiationParametersEntry ::= SEQUENCE {
 ipspSaNegParamName SnmpAdminString,
 ipspSaNegParamMinLifetimeSecs Unsigned32,
 ipspSaNegParamMinLifetimeKB Unsigned32,
 ipspSaNegParamRefreshThreshSecs Unsigned32,
 ipspSaNegParamRefreshThresholdKB Unsigned32,
 ipspSaNegParamIdleDurationSecs Unsigned32,
 ipspSaNegParamLastChanged TimeStamp,
 ipspSaNegParamStorageType StorageType,
 ipspSaNegParamRowStatus RowStatus
}

ipspSaNegParamName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "This object contains the administrative name of this
 SaNegotiationParametersEntry. This row can be referred
 to by this name in other policy action tables."
::= { ipspSaNegotiationParametersEntry 1 }

ipspSaNegParamMinLifetimeSecs OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "ipspSaNegParamMinLifetimeSecs specifies the minimum seconds
 lifetime that will be accepted from the peer."
::= { ipspSaNegotiationParametersEntry 2 }

ipspSaNegParamMinLifetimeKB OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "ipspSaNegParamMinLifetimeKB specifies the minimum kilobyte
 lifetime that will be accepted from the peer."
::= { ipspSaNegotiationParametersEntry 3 }

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

ipspSaNegParamRefreshThreshSecs OBJECT-TYPE

SYNTAX Unsigned32 (1..100)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipspSaNegParamRefreshThreshSecs 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 completely reached."

::= { ipspSaNegotiationParametersEntry 4 }

ipspSaNegParamRefreshThresholdKB OBJECT-TYPE

SYNTAX Unsigned32 (1..100)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipspSaNegParamRefreshThresholdKB 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."

::= { ipspSaNegotiationParametersEntry 5 }

ipspSaNegParamIdleDurationSecs OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipspSaNegParamIdleDurationSecs 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."

::= { ipspSaNegotiationParametersEntry 6 }

ipspSaNegParamLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or
created either through SNMP SETs or by some other external

Various Authors

[Page 60]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

means."
 ::= { ipspSaNegotiationParametersEntry 7 }

ipspSaNegParamStorageType 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."

DEFVAL { nonVolatile }
 ::= { ipspSaNegotiationParametersEntry 8 }

ipspSaNegParamRowStatus OBJECT-TYPE

SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the conceptual status of this row.

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

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

::= { ipspSaNegotiationParametersEntry 9 }

--
-- ipspIkeActionTable
--

ipspIkeActionTable OBJECT-TYPE

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

DESCRIPTION

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

::= { ipspConfigObjects 19 }

ipspIkeActionEntry OBJECT-TYPE
SYNTAX IpspIkeActionEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

Various Authors

[Page 61]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

"The ipspIkeActionEntry lists the IKE negotiation attributes."
INDEX { ipspIkeActName }
::= { ipspIkeActionTable 1 }

IpspIkeActionEntry ::= SEQUENCE {
ipspIkeActName SnmpAdminString,
ipspIkeActParametersName SnmpAdminString,
ipspIkeActThresholdDerivedKeys Integer32,
ipspIkeActExchangeMode INTEGER,
ipspIkeActAgressiveModeGroupId IkeGroupDescription,
ipspIkeActIdentityType IsecDoiIdentType,
ipspIkeActIdentityContext SnmpAdminString,
ipspIkeActPeerName SnmpAdminString,
ipspIkeActDoActionLogging TruthValue,
ipspIkeActDoPacketLogging IpspIPPacketLogging,
ipspIkeActVendorId OCTET STRING,
ipspIkeActLastChanged TimeStamp,
ipspIkeActStorageType StorageType,
ipspIkeActRowStatus RowStatus
}

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

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

ipspIkeActThresholdDerivedKeys OBJECT-TYPE
SYNTAX Integer32 (0..100)
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ipspIkeActThresholdDerivedKeys 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."

Various Authors

[Page 62]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

DEFVAL { 100 }
 ::= { ipspIkeActionEntry 3 }

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

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

ipspIkeActIdentityType OBJECT-TYPE

SYNTAX IpsecDoiIdentType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This column along with ipspIkeActIdentityContext and endpoint information is used to refer an ipspIkeIdentityEntry in the ipspIkeIdentityTable."
 ::= { ipspIkeActionEntry 6 }

ipspIkeActIdentityContext OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This column, along with ipspIkeActIdentityType and endpoint information, is used to refer to an ipspIkeIdentityEntry in the ipspIkeIdentityTable."
 ::= { ipspIkeActionEntry 7 }

ipspIkeActPeerName OBJECT-TYPE
SYNTAX SnmpAdminString(SIZE(0..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object indicates the peer id name of the IKE peer. This object can be used to look up the peer id value, address,

credentials and other values in the ipspPeerIdentityTable."
 ::= { ipspIkeActionEntry 8 }

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

ipspIkeActDoPacketLogging OBJECT-TYPE

SYNTAX IspIPPacketLogging
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ikeDoPacketLogging specifies whether or not an audit message should be logged and if there is logging, how many bytes of the packet to place in the notification."
DEFVAL { -1 }
 ::= { ipspIkeActionEntry 10 }

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

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

ipspIkeActStorageType 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."

```

DEFVAL { nonVolatile }
 ::= { ipspIkeActionEntry 13 }

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

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

    This object may not be set to destroy if referred to by other
    rows in other action tables."
 ::= { ipspIkeActionEntry 14 }

--
-- ipspIkeActionProposalsTable proposals contained within a ikeAction
--

ipspIkeActionProposalsTable OBJECT-TYPE
SYNTAX          SEQUENCE OF IpspIkeActionProposalsEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION
    "This table contains a list of all ike proposal names found
    within a given IKE Action."
 ::= { ipspConfigObjects 20 }

ipspIkeActionProposalsEntry OBJECT-TYPE
SYNTAX          IpspIkeActionProposalsEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION
    "a row containing one ike proposal reference"
INDEX          { ipspIkeActName, ipspIkeActPropPriority }
 ::= { ipspIkeActionProposalsTable 1 }

IpspIkeActionProposalsEntry ::= SEQUENCE {

```

```

    ipspIkeActPropName                SnmpAdminString,
    ipspIkeActPropLastChanged         TimeStamp,
    ipspIkeActPropStorageType         StorageType,
    ipspIkeActPropRowStatus           RowStatus
}

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

ipspIkeActPropName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The administratively assigned name that can be used to
         reference a set of values contained within the
         ipspIkeProposalTable."
    ::= { ipspIkeActionProposalsEntry 2 }

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

ipspIkeActPropStorageType 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."
    DEFVAL { nonVolatile }
    ::= { ipspIkeActionProposalsEntry 4 }

```

ipspIkeActPropRowStatus 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."

::= { ipspIkeActionProposalsEntry 5 }

--

-- IKE proposal definition table

--

ipspIkeProposalTable OBJECT-TYPE

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

"This table contains a list of IKE proposals which are used in an IKE negotiation."

::= { ipspConfigObjects 21 }

ipspIkeProposalEntry OBJECT-TYPE

SYNTAX IspIkeProposalEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

"One IKE proposal entry."

INDEX { ipspIkeActPropName }

::= { ipspIkeProposalTable 1 }

IspIkeProposalEntry ::= SEQUENCE {

ipspIkePropLifetimeDerivedKeys	Unsigned32,
ipspIkePropCipherAlgorithm	IkeEncryptionAlgorithm,
ipspIkePropCipherKeyLength	Unsigned32,
ipspIkePropCipherKeyRounds	Unsigned32,
ipspIkePropHashAlgorithm	IkeHashAlgorithm,
ipspIkePropPrfAlgorithm	INTEGER,
ipspIkePropVendorId	OCTET STRING,
ipspIkePropDhGroup	IkeGroupDescription,
ipspIkePropAuthenticationMethod	IkeAuthMethod,
ipspIkePropMaxLifetimeSecs	Unsigned32,
ipspIkePropMaxLifetimeKB	Unsigned32,

ipspIkePropProposalLastChanged
ipspIkePropProposalStorageType

TimeStamp,
StorageType,

Various Authors

[Page 67]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

ipspIkePropProposalRowStatus
}

RowStatus

ipspIkePropLifetimeDerivedKeys OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipspIkePropLifetimeDerivedKeys 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."

::= { ipspIkeProposalEntry 1 }

ipspIkePropCipherAlgorithm OBJECT-TYPE

SYNTAX IkeEncryptionAlgorithm

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspIkeProposalEntry 2 }

ipspIkePropCipherKeyLength OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspIkeProposalEntry 3 }

ipspIkePropCipherKeyRounds OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspIkeProposalEntry 4 }

ipspIkePropHashAlgorithm OBJECT-TYPE
SYNTAX IkeHashAlgorithm
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "ipspIkePropHashAlgorithm specifies the proposed phase 1
 security association hash algorithm."
 ::= { ipspIkeProposalEntry 5 }

Various Authors

[Page 68]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

ipspIkePropPrfAlgorithm OBJECT-TYPE
SYNTAX INTEGER { reserved(0) }
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "ipPRFAlgorithm specifies the proposed phase 1 security
 association psuedo-random function.

 Note: currently no prf algorithms are defined."
 ::= { ipspIkeProposalEntry 6 }

ipspIkePropVendorId 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."
 ::= { ipspIkeProposalEntry 7 }

ipspIkePropDhGroup OBJECT-TYPE
SYNTAX IkeGroupDescription
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "This object specifies the proposed phase 1 security
 association Diffie-Hellman group"
 ::= { ipspIkeProposalEntry 8 }

ipspIkePropAuthenticationMethod OBJECT-TYPE
SYNTAX IkeAuthMethod
MAX-ACCESS read-create

STATUS current
DESCRIPTION
"This object specifies the proposed authentication
method for the phase 1 security association."
 ::= { ipspIkeProposalEntry 9 }

ipspIkePropMaxLifetimeSecs OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ipspIkePropMaxLifetimeSecs specifies the maximum amount of
time to propose a security association remain valid.

A value of 0 indicates that the default lifetime of
8 hours should be used."

Various Authors

[Page 69]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

::= { ipspIkeProposalEntry 10 }

ipspIkePropMaxLifetimeKB OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ipspIkePropMaxLifetimeKB specifies the maximum kilobyte
lifetime to propose a security association remain valid."
 ::= { ipspIkeProposalEntry 11 }

ipspIkePropProposalLastChanged OBJECT-TYPE

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

ipspIkePropProposalStorageType 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."

DEFVAL { nonVolatile }
 ::= { ipspIkeProposalEntry 13 }

ipspIkePropProposalRowStatus 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."

::= { ipspIkeProposalEntry 14 }

--

-- IPsec action definition table

--

Various Authors

[Page 70]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

ipspIpsecActionTable OBJECT-TYPE

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

DESCRIPTION

"The ipspIpsecActionTable contains a list of the parameters used for an IKE phase 2 IPsec DOI negotiation."

::= { ipspConfigObjects 22 }

ipspIpsecActionEntry OBJECT-TYPE

SYNTAX IspIpsecActionEntry
MAX-ACCESS not-accessible
STATUS current

DESCRIPTION

"The ipspIpsecActionEntry lists the IPsec negotiation attributes."

INDEX { ipspIpsecActName }
 ::= { ipspIpsecActionTable 1 }


```

IpspIpssecActionEntry ::= SEQUENCE {
    ipspIpssecActName                SnmpAdminString,
    ipspIpssecActParametersName      SnmpAdminString,
    ipspIpssecActProposalsName       SnmpAdminString,
    ipspIpssecActUsePfs               TruthValue,
    ipspIpssecActVendorId            OCTET STRING,
    ipspIpssecActGroupId              IkeGroupDescription,
    ipspIpssecActPeerGatewayIdName   OCTET STRING,
    ipspIpssecActUseIkeGroup         TruthValue,
    ipspIpssecActGranularity          INTEGER,
    ipspIpssecActMode                 INTEGER,
    ipspIpssecActDFHandling           INTEGER,
    ipspIpssecActDoActionLogging     TruthValue,
    ipspIpssecActDoPacketLogging     IpspIPPacketLogging,
    ipspIpssecActLastChanged         TimeStamp,
    ipspIpssecActStorageType          StorageType,
    ipspIpssecActRowStatus            RowStatus
}

```

```

ipspIpssecActName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "ipspIpssecActName is the name of the ipsecAction entry."
    ::= { ipspIpssecActionEntry 1 }

```

```

ipspIpssecActParametersName OBJECT-TYPE

```

Various Authors

[Page 71]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

```

SYNTAX      SnmpAdminString (SIZE(1..32))
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION

```

```

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

```

```

::= { ipspIpssecActionEntry 2 }

```

```

ipspIpssecActProposalsName OBJECT-TYPE

```

```

    SYNTAX      SnmpAdminString (SIZE(1..32))

```

MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object is used to reference one or more rows in the
 ipspIpsecProposalsTable where an ordered list of proposals
 affecting this action may be found."
 ::= { ipspIpsecActionEntry 3 }

ipspIpsecActUsePfs 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."
 ::= { ipspIpsecActionEntry 4 }

ipspIpsecActVendorId 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."
 ::= { ipspIpsecActionEntry 5 }

ipspIpsecActGroupId OBJECT-TYPE
SYNTAX IkeGroupDescription
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This object specifies the Diffie-Hellman group to use for
 phase 2 when the object ipspIpsecActUsePfs is true and the
 object ipspIpsecActUseIkeGroup is false. If the GroupID
 number is from the vendor-specific range (32768-65535), the
 VendorID qualifies the group number."

::= { ipspIpsecActionEntry 6 }

ipspIpsecActPeerGatewayIdName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..116))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspIpsecActionEntry 7 }

ipspIpsecActUseIkeGroup OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspIpsecActionEntry 8 }

ipspIpsecActGranularity OBJECT-TYPE

SYNTAX INTEGER { subnet(1), address(2), protocol(3),
port(4) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies how the proposed selector for the security association will be created. The selector is created by using the FilterList information. The selector can be subnet, address, porotocol, or port."

::= { ipspIpsecActionEntry 9 }

ipspIpsecActMode OBJECT-TYPE

SYNTAX INTEGER { tunnel(1), transport(2) }

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies the encapsulation of the IPsec SA to be negotiated."

DEFVAL { tunnel }

::= { ipspIpsecActionEntry 10 }

ipspIpsecActDFHandling 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."

DEFVAL { copy }

::= { ipspIpsecActionEntry 11 }

ipspIpsecActDoActionLogging OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipspIpsecActDoActionLogging specifies whether or not an audit message should be logged when this ipsec SA is created."

DEFVAL { false }

::= { ipspIpsecActionEntry 12 }

ipspIpsecActDoPacketLogging OBJECT-TYPE

SYNTAX IpspIPPacketLogging

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"ipspIpsecActDoPacketLogging specifies whether or not an audit message should be logged and if there is logging, how many bytes of the packet to place in the notification."

DEFVAL { -1 }

::= { ipspIpsecActionEntry 13 }

ipspIpsecActLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

::= { ipspIpsecActionEntry 14 }

ipspIpsecActStorageType OBJECT-TYPE

SYNTAX StorageType

MAX-ACCESS read-create

STATUS current

Various Authors

[Page 74]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

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."

DEFVAL { nonVolatile }

::= { ipspIpsecActionEntry 15 }

ipspIpsecActRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

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

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

::= { ipspIpsecActionEntry 16 }

--

-- ipspIpsecProposalsTable

--

ipspIpsecProposalsTable OBJECT-TYPE

SYNTAX SEQUENCE OF IspIpsecProposalsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

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

::= { ipspConfigObjects 23 }

ipspIpsecProposalsEntry OBJECT-TYPE

SYNTAX IspIpsecProposalsEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An entry containing (possibly a portion of) a proposal."
INDEX { ipspIpssecPropName, ipspIpssecPropPriority,
ipspIpssecPropProtocolId }
 ::= { ipspIpssecProposalsTable 1 }

IpspIpssecProposalsEntry ::= SEQUENCE {
 ipspIpssecPropName SnmpAdminString,
 ipspIpssecPropPriority Integer32,

Various Authors

[Page 75]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

ipspIpssecPropProtocolId IpsecDoiSecProtocolId,
 ipspIpssecPropTransformsName SnmpAdminString,
 ipspIpssecPropLastChanged TimeStamp,
 ipspIpssecPropStorageType StorageType,
 ipspIpssecPropRowStatus RowStatus
 }

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

ipspIpssecPropPriority OBJECT-TYPE
 SYNTAX Integer32 (0..65535)
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 "The priority level (AKA sequence level) of this proposal.
 A lower number indicates a higher precedence."
 ::= { ipspIpssecProposalsEntry 2 }

ipspIpssecPropProtocolId OBJECT-TYPE
 SYNTAX IpsecDoiSecProtocolId
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 "The protocol Id for the transforms for this proposal. The
 protoIsakmp(1) value is not valid for this object.
 This object, along with the ipspIpssecPropTransformsName,
 is the index into the ipspIpssecTransformsTable."

```
::= { ipspIpsecProposalsEntry 3 }
```

```
ipspIpsecPropTransformsName OBJECT-TYPE
```

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

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

```
STATUS      current
```

```
DESCRIPTION
```

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

```
::= { ipspIpsecProposalsEntry 4 }
```

```
ipspIpsecPropLastChanged OBJECT-TYPE
```

```
SYNTAX      TimeStamp
```

Various Authors

[Page 76]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

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

```
STATUS      current
```

```
DESCRIPTION
```

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

```
::= { ipspIpsecProposalsEntry 5 }
```

```
ipspIpsecPropStorageType 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."
```

```
DEFVAL { nonVolatile }
```

```
::= { ipspIpsecProposalsEntry 6 }
```

```
ipspIpsecPropRowStatus OBJECT-TYPE
```

```
SYNTAX      RowStatus
```

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

```
STATUS      current
```

```
DESCRIPTION
```

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

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

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

```
::= { ipspIpssecProposalsEntry 7 }
```

```
--
```

```
-- ipspIpssecTransformsTable
```

```
--
```

```
ipspIpssecTransformsTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF IpspIpssecTransformsEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

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

```
::= { ipspConfigObjects 24 }
```

Various Authors

[Page 77]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

```
ipspIpssecTransformsEntry OBJECT-TYPE
```

```
SYNTAX IpspIpssecTransformsEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

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

```
INDEX { ipspIpssecTranType, ipspIpssecTranName,  
 ipspIpssecTranPriority }
```

```
::= { ipspIpssecTransformsTable 1 }
```

```
IpspIpssecTransformsEntry ::= SEQUENCE {
```

```
 ipspIpssecTranType IpsecDoiSecProtocolId,  
 ipspIpssecTranName SnmpAdminString,  
 ipspIpssecTranPriority Integer32,  
 ipspIpssecTranTransformName SnmpAdminString,  
 ipspIpssecTranLastChanged TimeStamp,  
 ipspIpssecTranStorageType StorageType,  
 ipspIpssecTranRowStatus RowStatus
```

```
}
```


ipspIpssecTranType OBJECT-TYPE
SYNTAX IpsecDoiSecProtocolId
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The protocol type for this transform. The protoIsakmp(1)
value is not valid for this object."
 ::= { ipspIpssecTransformsEntry 1 }

ipspIpssecTranName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The name for this transform or group of transforms."
 ::= { ipspIpssecTransformsEntry 2 }

ipspIpssecTranPriority OBJECT-TYPE
SYNTAX Integer32 (0..65535)
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The priority level (AKA sequence level) of the this transform
within the group of transforms. This indicates the
preference for which algorithms are requested when the list
of transforms are sent to the remote host. A lower number
indicates a higher precedence."
 ::= { ipspIpssecTransformsEntry 3 }

ipspIpssecTranTransformName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(1..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The name for the given transform. Depending on the value of
ipspIpssecTranType, this value should be used to lookup the
transform's specific parameters in the ipspAhTransformTable,
the ipspEspTransformTable or the ipspIpcompTransformTable."
 ::= { ipspIpssecTransformsEntry 4 }

ipspIpssecTranLastChanged OBJECT-TYPE

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

ipspIpsecTranStorageType 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."
DEFVAL { nonVolatile }
 ::= { ipspIpsecTransformsEntry 6 }

ipspIpsecTranRowStatus OBJECT-TYPE

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

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

 This row may not be set to active until the corresponding row
 in the ipspAhTransformTable, ipspEspTransformTable or the
 ipspIpcompTransformTable exists."
 ::= { ipspIpsecTransformsEntry 7 }

```

ipspAhTransformTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IspAhTransformEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table lists all the AH transforms which can be used to
        build IPsec proposals."
    ::= { ipspConfigObjects 25 }

```

```

ipspAhTransformEntry OBJECT-TYPE
    SYNTAX      IspAhTransformEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This entry contains the attributes of one AH transform."
    INDEX       { ipspAhTranName }
    ::= { ipspAhTransformTable 1 }

```

```

IspAhTransformEntry ::= SEQUENCE {
    ipspAhTranName           SnmpAdminString,
    ipspAhTranMaxLifetimeSec Unsigned32,
    ipspAhTranMaxLifetimeKB Unsigned32,
    ipspAhTranAlgorithm     IspAhAuthAlgorithm,
    ipspAhTranReplayProtection TruthValue,
    ipspAhTranReplayWindowSize Unsigned32,
    ipspAhTranLastChanged   TimeStamp,
    ipspAhTranStorageType   StorageType,
    ipspAhTranRowStatus     RowStatus
}

```

```

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

```

```

ipspAhTranMaxLifetimeSec OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-create
    STATUS      current

```

DESCRIPTION

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

A value of 0 indicates that the default lifetime of 8 hours should be used."

::= { ipspAhTransformEntry 2 }

ipspAhTranMaxLifetimeKB OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspAhTransformEntry 3 }

ipspAhTranAlgorithm OBJECT-TYPE

SYNTAX IpsecDoiAuthAlgorithm

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object specifies the AH algorithm for this transform."

::= { ipspAhTransformEntry 4 }

ipspAhTranReplayProtection OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspAhTransformEntry 5 }

ipspAhTranReplayWindowSize OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspAhTransformEntry 6 }

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

ipspAhTranLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

::= { ipspAhTransformEntry 7 }

ipspAhTranStorageType 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."

DEFVAL { nonVolatile }

::= { ipspAhTransformEntry 8 }

ipspAhTranRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

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

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

::= { ipspAhTransformEntry 9 }

--

-- ESP transform definition table

--

ipspEspTransformTable OBJECT-TYPE

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

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

Various Authors

[Page 82]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

::= { ipspConfigObjects 26 }

ipspEspTransformEntry OBJECT-TYPE

SYNTAX IspEspTransformEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

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

INDEX { ipspEspTranName }

::= { ipspEspTransformTable 1 }

IspEspTransformEntry ::= SEQUENCE {

ipspEspTranName	SnmpAdminString,
ipspEspTranMaxLifetimeSec	Unsigned32,
ipspEspTranMaxLifetimeKB	Unsigned32,
ipspEspTranCipherTransformId	IpsecDoiEspTransform,
ipspEspTranCipherKeyLength	Unsigned32,
ipspEspTranCipherKeyRounds	Unsigned32,
ipspEspTranIntegrityAlgorithmId	IpsecDoiAuthAlgorithm,
ipspEspTranReplayPrevention	TruthValue,
ipspEspTranReplayWindowSize	Unsigned32,
ipspEspTranLastChanged	TimeStamp,
ipspEspTranStorageType	StorageType,
ipspEspTranRowStatus	RowStatus

}

ipspEspTranName OBJECT-TYPE

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

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

::= { ipspEspTransformEntry 1 }

ipspEspTranMaxLifetimeSec OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION

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

A value of 0 indicates that the default lifetime of 8 hours should be used."

::= { ipspEspTransformEntry 2 }

ipspEspTranMaxLifetimeKB OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION

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

::= { ipspEspTransformEntry 3 }

ipspEspTranCipherTransformId OBJECT-TYPE

SYNTAX IpsecDoiEspTransform
MAX-ACCESS read-create
STATUS current
DESCRIPTION

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

::= { ipspEspTransformEntry 4 }

ipspEspTranCipherKeyLength OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION

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

::= { ipspEspTransformEntry 5 }

ipspEspTranCipherKeyRounds OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object specifies the number of key rounds for the ESP cipher algorithm."

::= { ipspEspTransformEntry 6 }

ipspEspTranIntegrityAlgorithmId OBJECT-TYPE

SYNTAX IpsecDoiAuthAlgorithm
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object specifies the ESP integrity algorithm ID."

::= { ipspEspTransformEntry 7 }

ipspEspTranReplayPrevention OBJECT-TYPE

SYNTAX TruthValue

Various Authors

[Page 84]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

MAX-ACCESS read-create
STATUS current
DESCRIPTION

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

::= { ipspEspTransformEntry 8 }

ipspEspTranReplayWindowSize OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION

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

::= { ipspEspTransformEntry 9 }

ipspEspTranLastChanged OBJECT-TYPE

SYNTAX TimeStamp


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

```
ipspEspTranStorageType 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."
DEFVAL { nonVolatile }
 ::= { ipspEspTransformEntry 11 }
```

```
ipspEspTranRowStatus 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
```

Various Authors

[Page 85]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

objects in this conceptual row can be modified.

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

```
 ::= { ipspEspTransformEntry 12 }
```

--

-- IP compression transform definition table

--

```
ipspIpcompTransformTable OBJECT-TYPE
SYNTAX SEQUENCE OF IpspIpcompTransformEntry
```

```

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."
 ::= { ipspConfigObjects 27 }

```

```

ipspIpcompTransformEntry OBJECT-TYPE
SYNTAX IpspIpcompTransformEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
    "This entry contains the attributes of one IP compression
    transform."
INDEX { ipspIpcompTranName }
 ::= { ipspIpcompTransformTable 1 }

```

```

IpspIpcompTransformEntry ::= SEQUENCE {
    ipspIpcompTranName                SnmpAdminString,
    ipspIpcompTranMaxLifetimeSec      Unsigned32,
    ipspIpcompTranMaxLifetimeKB      Unsigned32,
    ipspIpcompTranAlgorithm           IsecDoiIpcompTransform,
    ipspIpcompTranDictionarySize      Unsigned32,
    ipspIpcompTranPrivateAlgorithm    Unsigned32,
    ipspIpcompTranLastChanged         TimeStamp,
    ipspIpcompTranStorageType         StorageType,
    ipspIpcompTranRowStatus           RowStatus
}

```

```

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

```

```

DESCRIPTION
    "The name of this ipspIpcompTransformEntry."
 ::= { ipspIpcompTransformEntry 1 }

```

```

ipspIpcompTranMaxLifetimeSec OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS read-create

```

STATUS current
DESCRIPTION
"ipspIpcompTranMaxLifetimeSec specifies how long in seconds the security association derived from this transform should be used.

A value of 0 indicates that the default lifetime of 8 hours should be used."
 ::= { ipspIpcompTransformEntry 2 }

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

ipspIpcompTranAlgorithm OBJECT-TYPE
SYNTAX IpsecDoiIpcompTransform
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"ipspIpcompTranAlgorithm specifies the transform ID of the IP compression algorithm."
 ::= { ipspIpcompTransformEntry 4 }

ipspIpcompTranDictionarySize OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"If the algorithm in ipspIpcompTranAlgorithm 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."
 ::= { ipspIpcompTransformEntry 5 }

ipspIpcompTranPrivateAlgorithm OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"If ipspIpcompTranPrivateAlgorithm has a value other zero,
then it is up to the vendors implementation to determine the
meaning of this field and substitute a data compression
algorithm in place of ipspIpcompTranAlgorithm."
 ::= { ipspIpcompTransformEntry 6 }

ipspIpcompTranLastChanged OBJECT-TYPE

SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or
created either through SNMP SETs or by some other external
means."
 ::= { ipspIpcompTransformEntry 7 }

ipspIpcompTranStorageType 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."
DEFVAL { nonVolatile }
 ::= { ipspIpcompTransformEntry 8 }

ipspIpcompTranRowStatus OBJECT-TYPE

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

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

If active, this object must remain active if it is referenced
by a row in another table."
 ::= { ipspIpcompTransformEntry 9 }

--

-- IKE identity definition table

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

--

ipspIkeIdentityTable OBJECT-TYPE

SYNTAX SEQUENCE OF IspIkeIdentityEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"IKEIdentity is used to represent the identities that may be used for an IPProtocolEndpoint (or collection of IPProtocolEndpoints) to identify itself in IKE phase 1 negotiations. The column ikeIdentityName in an ipspIkeActionEntry together with the ipspEndGroupIdentType and the ipspEndGroupAddress in the PolicyEndpointToGroupTable specifies the unique identity to use in a negotiation exchange."

::= { ipspConfigObjects 28 }

ipspIkeIdentityEntry OBJECT-TYPE

SYNTAX IspIkeIdentityEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"ikeIdentity lists the attributes of an IKE identity."

INDEX { ipspEndGroupIdentType, ipspEndGroupAddress,
 ipspIkeActIdentityType, ipspIkeActIdentityContext }

::= { ipspIkeIdentityTable 1 }

IspIkeIdentityEntry ::= SEQUENCE {

ipspIkeIdCredentialName SnmpAdminString,

ipspIkeIdLastChanged TimeStamp,

ipspIkeIdStorageType StorageType,

ipspIkeIdRowStatus RowStatus

}

ipspIkeIdCredentialName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This value is used as an index into the ipspCredentialTable to look up the actual credential value and other credential information."

For ID's without associated credential information, this value is left blank.

For ID's that are address types, this value may be left blank

and the associated IPProtocolEndpoint or appropriate member of the Collection of endpoints is used."

::= { ipspIkeIdentityEntry 1 }

ipspIkeIdLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

::= { ipspIkeIdentityEntry 2 }

ipspIkeIdStorageType 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."

DEFVAL { nonVolatile }

::= { ipspIkeIdentityEntry 3 }

ipspIkeIdRowStatus OBJECT-TYPE

SYNTAX RowStatus

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object indicates the conceptual status of this row.

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

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

```
    by a row in another table."
 ::= { ipspIkeIdentityEntry 4 }
```

```
--
-- Peer Identity Table
--
```

```
ipspPeerIdentityTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IspspPeerIdentityEntry
    MAX-ACCESS  not-accessible
```

Various Authors

[Page 90]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

```
STATUS      current
DESCRIPTION
    "PeerIdentity is used to represent the identities that may be
    used for peers to identify themselves in IKE phase I/II
    negotiations. PeerIdentityTable aggregates the table entries
    that provide mappings between identities and their
    addresses."
 ::= { ipspConfigObjects 29 }
```

```
ipspPeerIdentityEntry OBJECT-TYPE
    SYNTAX      IspspPeerIdentityEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "peerIdentity matches a peer's identity to its address."
    INDEX { ipspPeerIdName, ipspPeerIdPriority }
    ::= { ipspPeerIdentityTable 1 }
```

```
IspspPeerIdentityEntry ::= SEQUENCE {
    ipspPeerIdName          SnmpAdminString,
    ipspPeerIdPriority      Integer32,
    ipspPeerIdType         IspsecDoiIdentType,
    ipspPeerIdValue        IspspIdentityFilter,
    ipspPeerIdAddressType  InetAddressType,
    ipspPeerIdAddress      InetAddress,
    ipspPeerIdCredentialName SnmpAdminString,
    ipspPeerIdLastChanged  TimeStamp,
    ipspPeerIdStorageType  StorageType,
    ipspPeerIdRowStatus    RowStatus
```

```
}
```

```
ipspPeerIdName OBJECT-TYPE
  SYNTAX      SnmpAdminString (SIZE(1..32))
  MAX-ACCESS  not-accessible
  STATUS      current
  DESCRIPTION
    "This is an administratively assigned value that, together
    with ipspPeerIdPriority, uniquely identifies an entry in this
    table."
  ::= { ipspPeerIdentityEntry 1 }
```

```
ipspPeerIdPriority OBJECT-TYPE
  SYNTAX      Integer32 (0..2147483647)
  MAX-ACCESS  not-accessible
  STATUS      current
  DESCRIPTION
    "This object, along with ipspPeerIdName, uniquely identifies an
    entry in this table. The priority also indicates the order
```

Various Authors

[Page 91]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

```
    of peer gateways to initiate or accept SAs from (i.e. try
    until success)."
```

```
::= { ipspPeerIdentityEntry 2 }
```

```
ipspPeerIdType            OBJECT-TYPE
  SYNTAX            IpsecDoiIdentType
  MAX-ACCESS        read-create
  STATUS            current
  DESCRIPTION
    "ipspPeerIdType is an enumeration identifying the type of the
    Identity value."
  ::= { ipspPeerIdentityEntry 3 }
```

```
ipspPeerIdValue         OBJECT-TYPE
  SYNTAX            IpspIdentityFilter
  MAX-ACCESS        read-create
  STATUS            current
  DESCRIPTION
    "ipspPeerIdValue contains an Identity filter to be used to match
    against the identity payload in an IKE request. If this value
    matches the value in the identity payload, the credential for
    the peer can be found using the ipspPeerIdCredentialName as
```


an index into the credential table."
 ::= { ipspPeerIdentityEntry 4 }

ipspPeerIdAddressType OBJECT-TYPE

SYNTAX InetAddressType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The property ipspPeerIdAddressType specifies the format of the ipspPeerIdAddress property value."

::= { ipspPeerIdentityEntry 5 }

ipspPeerIdAddress OBJECT-TYPE

SYNTAX InetAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

Values of unknown, ipv4z, ipv6z and dns are not legal values for this object."

::= { ipspPeerIdentityEntry 6 }

ipspPeerIdCredentialName OBJECT-TYPE

SYNTAX SnmpAdminString (SIZE(0..32))

Various Authors

[Page 92]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

MAX-ACCESS read-create

STATUS current

DESCRIPTION

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

::= { ipspPeerIdentityEntry 7 }

ipspPeerIdLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

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

```

        created either through SNMP SETs or by some other external
        means."
 ::= { ipspPeerIdentityEntry 8 }

ipspPeerIdStorageType 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."
    DEFVAL { nonVolatile }
 ::= { ipspPeerIdentityEntry 9 }

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

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

        If active, this object must remain active if it is referenced
        by a row in another table."
 ::= { ipspPeerIdentityEntry 10 }

--
-- autostart IKE Table
--
```

```

ipspAutostartIkeTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IspAutostartIkeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The parameters in the autostart IKE Table are used to
        automatically initiate IKE phaes I and II (i.e. IPsec)
        negotiations on startup.  It also will initiate IKE phase I
```

```

        and II negotiations for a row at the time of that row's
        creation"
 ::= { ipspConfigObjects 30 }

ipspAutostartIkeEntry OBJECT-TYPE
    SYNTAX      IspAutostartIkeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "autostart ike provides the set of parameters to automatically
        start IKE and IPsec SA's."
    INDEX { ipspAutoIkePriority }
    ::= { ipspAutostartIkeTable 1 }

IspAutostartIkeEntry ::= SEQUENCE {
    ipspAutoIkePriority          Integer32,
    ipspAutoIkeAction           VariablePointer,
    ipspAutoIkeAddressType     InetAddressType,
    ipspAutoIkeSourceAddress    InetAddress,
    ipspAutoIkeSourcePort      InetPortNumber,
    ipspAutoIkeDestAddress     InetAddress,
    ipspAutoIkeDestPort        InetPortNumber,
    ipspAutoIkeProtocol        Unsigned32,
    ipspAutoIkeLastChanged     TimeStamp,
    ipspAutoIkeStorageType     StorageType,
    ipspAutoIkeRowStatus       RowStatus
}

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

ipspAutoIkeAction OBJECT-TYPE
    SYNTAX      VariablePointer
    MAX-ACCESS  read-create

```

DESCRIPTION

"This pointer is used to point to the action or compound action that should be initiated by this row."

::= { ipspAutostartIkeEntry 2 }

ipspAutoIkeAddressType OBJECT-TYPE

SYNTAX InetAddressType

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The property ipspAutoIkeAddressType specifies the format of the autoIke source and destination Address values.

Values of unknown, ipv4z, ipv6z and dns are not legal values for this object."

::= { ipspAutostartIkeEntry 3 }

ipspAutoIkeSourceAddress OBJECT-TYPE

SYNTAX InetAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The property autoIkeSourecAddress specifies Source IP address for autostarting IKE SA's, formatted according to the appropriate convention as defined in the ipspAutoIkeAddressType property."

::= { ipspAutostartIkeEntry 4 }

ipspAutoIkeSourcePort OBJECT-TYPE

SYNTAX InetPortNumber

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The property ipspAutoIkeSourcePort specifies the port number for the source port for autostarting IKE SA's.

The value of 0 for this object is illegal."

::= { ipspAutostartIkeEntry 5 }

ipspAutoIkeDestAddress OBJECT-TYPE

SYNTAX InetAddress

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The property ipspAutoIkeDestAddress specifies the Destination IP address for autostarting IKE SA's, formatted according to the appropriate convention as defined in the

```
    ipspAutoIkeAddressType property."  
 ::= { ipspAutostartIkeEntry 6 }
```

```
ipspAutoIkeDestPort OBJECT-TYPE
```

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

```
    "The property ipspAutoIkeDestPort specifies the port number for  
    the destination port for autostarting IKE SA's.
```

```
    The value of 0 for this object is illegal."
```

```
 ::= { ipspAutostartIkeEntry 7 }
```

```
ipspAutoIkeProtocol OBJECT-TYPE
```

```
SYNTAX      Unsigned32 (0..255)  
MAX-ACCESS  read-create  
STATUS      current  
DESCRIPTION
```

```
    "The property Protocol specifies the protocol number used in  
    comparing with policy filter entries and used in any phase 2  
    negotiations."
```

```
 ::= { ipspAutostartIkeEntry 8 }
```

```
ipspAutoIkeLastChanged OBJECT-TYPE
```

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

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

```
 ::= { ipspAutostartIkeEntry 9 }
```

```
ipspAutoIkeStorageType 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."
```

```
DEFVAL { nonVolatile }
```

```
 ::= { ipspAutostartIkeEntry 10 }
```

```
ipspAutoIkeRowStatus OBJECT-TYPE
```

SYNTAX RowStatus
MAX-ACCESS read-create

Various Authors

[Page 96]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

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."

::= { ipspAutostartIkeEntry 11 }

--
-- CA Table
--

ipspIpsecCredMngServiceTable OBJECT-TYPE
SYNTAX SEQUENCE OF IspIpsecCredMngServiceEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "A table of Credential Management Service values. This table
 is usually used for credential/certificate values that are
 used with a management service (e.g. Certificate
 Authorities)."
::= { ipspConfigObjects 31 }

ipspIpsecCredMngServiceEntry OBJECT-TYPE
SYNTAX IspIpsecCredMngServiceEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "A row in the ipspIpsecCredMngServiceTable."
INDEX { ipspIcmsName }
::= { ipspIpsecCredMngServiceTable 1 }

IspIpsecCredMngServiceEntry ::= SEQUENCE {
 ipspIcmsName SnmpAdminString,
 ipspIcmsDistinguishedName OCTET STRING,
 ipspIcmsPolicyStatement OCTET STRING,
 ipspIcmsMaxChainLength Integer32,

```
    ipspIcmsCredentialName      SnmpAdminString,
    ipspIcmsLastChanged         TimeStamp,
    ipspIcmsStorageType         StorageType,
    ipspIcmsRowStatus           RowStatus
}
```

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

Various Authors

[Page 97]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

```
STATUS      current
DESCRIPTION
    "This is an administratively assigned string used to index
    this table."
 ::= { ipspIpsecCredMngServiceEntry 1 }
```

```
ipspIcmsDistinguishedName OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(1..256))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This value represents the Distinguished Name of the
        Credential Management Service."
 ::= { ipspIpsecCredMngServiceEntry 2 }
```

```
ipspIcmsPolicyStatement OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..1024))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This Value represents the Credential Management Service
        Policy Statement, or a reference describing how to obtain it
        (e.g., a URL).  If one doesn't exist, this value can be left
        blank"
 ::= { ipspIpsecCredMngServiceEntry 3 }
```

```
ipspIcmsMaxChainLength OBJECT-TYPE
    SYNTAX      Integer32 (0..255)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This value is the maximum length of the chain allowable from
```

the Credential Management Service to the credential in question."
DEFVAL { 0 }
::= { ipspIpsecCredMngServiceEntry 4 }

ipspIcmsCredentialName OBJECT-TYPE
SYNTAX SnmpAdminString (SIZE(0..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This value is used as an index into the ipspCredentialTable to look up the actual credential value."
::= { ipspIpsecCredMngServiceEntry 5 }

ipspIcmsLastChanged OBJECT-TYPE
SYNTAX TimeStamp

Various Authors

[Page 98]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The value of sysUpTime when this row was last modified or created either through SNMP SETs or by some other external means."
::= { ipspIpsecCredMngServiceEntry 6 }

ipspIcmsStorageType 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."
DEFVAL { nonVolatile }
::= { ipspIpsecCredMngServiceEntry 7 }

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

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

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

```
::= { ipspIpssecCredMngServiceEntry 8 }
```

```
--
```

```
-- CRL Table
```

```
--
```

```
ipspCredMngCRLTable OBJECT-TYPE
```

```
SYNTAX SEQUENCE OF IpspCredMngCRLEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"A table of the Credential Revocation Lists (CRL) for credential management services."
```

```
::= { ipspConfigObjects 32 }
```

```
ipspCredMngCRLEntry OBJECT-TYPE
```

Various Authors

[Page 99]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

```
SYNTAX IpspCredMngCRLEntry
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"A row in the ipspCredMngCRLTable."
```

```
INDEX { ipspIcmsName , ipspCmcCRLName }
```

```
::= { ipspCredMngCRLTable 1 }
```

```
IpspCredMngCRLEntry ::= SEQUENCE {
```

```
    ipspCmcCRLName SnmpAdminString,
```

```
    ipspCmcDistributionPoint OCTET STRING,
```

```
    ipspCmcThisUpdate OCTET STRING,
```

```
    ipspCmcNextUpdate OCTET STRING,
```

```
    ipspCmcLastChanged TimeStamp,
```

```
    ipspCmcStorageType StorageType,
```

```
    ipspCmcRowStatus RowStatus
```

```
}
```

ipspCmcCRLName OBJECT-TYPE
SYNTAX SnmpAdminString(SIZE(1..32))
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"This is an administratively assigned string used to index
this table. It represents a CRL for a given CA from a given
distribution point."
 ::= { ipspCredMngCRLEntry 1 }

ipspCmcDistributionPoint OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..256))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This Value represents a Distribution Point for a Credential
Revocation List. It can be relative to the Credential
Management Service or a full name (URL, e-mail, etc...)."
 ::= { ipspCredMngCRLEntry 2 }

ipspCmcThisUpdate OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This value is the issue date of this CRL. This
should be in utctime or generalizedtime."
 ::= { ipspCredMngCRLEntry 3 }

ipspCmcNextUpdate OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..32))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"This value indicates the date the next version of this CRL
will be issued. This should be in utctime or
generalizedtime."
 ::= { ipspCredMngCRLEntry 4 }

ipspCmcLastChanged OBJECT-TYPE
SYNTAX TimeStamp

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

```
ipspCmcStorageType 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."
DEFVAL { nonVolatile }
 ::= { ipspCredMngCRLEntry 6 }
```

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

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

    If active, this object must remain active if it is referenced
    by a row in another table."
 ::= { ipspCredMngCRLEntry 7 }
```

```
--
-- Revoked Certificate Table
--
```

```
ipspRevokedCertificateTable OBJECT-TYPE
SYNTAX SEQUENCE OF IpspRevokedCertificateEntry
MAX-ACCESS not-accessible
STATUS current
```

DESCRIPTION

"A table of Credentials revoked by credential management services. That is, this table is a table of Certificates that are on CRL's, Credential Revocation Lists."

::= { ipspConfigObjects 33 }

ipspRevokedCertificateEntry OBJECT-TYPE

SYNTAX IpspRevokedCertificateEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"A row in the ipspRevokedCertificateTable."

INDEX { ipspCmcCRLName, ipspRctCertSerialNumber}

::= { ipspRevokedCertificateTable 1 }

IpspRevokedCertificateEntry ::= SEQUENCE {

ipspRctCertSerialNumber Unsigned32,
ipspRctRevokedDate OCTET STRING,
ipspRctRevokedReason INTEGER,
ipspRctLastChanged TimeStamp,
ipspRctStorageType StorageType,
ipspRctRowStatus RowStatus

}

ipspRctCertSerialNumber OBJECT-TYPE

SYNTAX Unsigned32 (0..4294967295)

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"This value is the serial number of the revoked certificate."

::= { ipspRevokedCertificateEntry 1 }

ipspRctRevokedDate OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..32))

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This value is the revocation date of the certificate. This should be in utctime or generaltime."

::= { ipspRevokedCertificateEntry 2 }

ipspRctRevokedReason OBJECT-TYPE

SYNTAX INTEGER { reserved(0), unspecified(1), keyCompromise(2),
cACompromise(3), affiliationChanged(4),

```

        superseded(5), cessationOfOperation(6),
        certificateHold(7), removeFromCRL(8) }
MAX-ACCESS    read-create
STATUS        current
DESCRIPTION
    "This value is the reason this certificate was revoked."
DEFVAL        { unspecified }
 ::= { ipspRevokedCertificateEntry 3 }

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

ipspRctStorageType 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."
DEFVAL { nonVolatile }
 ::= { ipspRevokedCertificateEntry 5 }

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

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

    If active, this object must remain active if it is referenced
    by a row in another table."
 ::= { ipspRevokedCertificateEntry 6 }

--
-- Credential Table
```

ipspCredentialTable OBJECT-TYPE
SYNTAX SEQUENCE OF IppspCredentialEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "A table of credential values. Example of Credentials are
 shared secrets, certificates or kerberos tickets."
 ::= { ipspConfigObjects 34 }

ipspCredentialEntry OBJECT-TYPE
SYNTAX IppspCredentialEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "A row in the ipspCredentialTable."
INDEX { ipspCredName }
 ::= { ipspCredentialTable 1 }

IppspCredentialEntry ::= SEQUENCE {
 ipspCredName SnmpAdminString,
 ipspCredType IppspCredentialType,
 ipspCredCredential OCTET STRING,
 ipspCredSize Integer32,
 ipspCredMngName SnmpAdminString,
 ipspCredRemoteID OCTET STRING,
 ipspCredAdminStatus IppspAdminStatus,
 ipspCredLastChanged TimeStamp,
 ipspCredStorageType StorageType,
 ipspCredRowStatus RowStatus
}

ipspCredName OBJECT-TYPE
SYNTAX SnmpAdminString(SIZE(1..32))
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
 "This object represents the name for an entry in this table."
 ::= { ipspCredentialEntry 1 }

ipspCredType OBJECT-TYPE

SYNTAX IpspCredentialType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "This object represents the type of the credential for this
 row."
 ::= { ipspCredentialEntry 2 }

Various Authors

[Page 104]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

ipspCredCredential OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..1024))
MAX-ACCESS read-create
STATUS current
DESCRIPTION
 "This object represents the credential value.

If the size of the credential is greater than 1024, the credential must be configured via the ipspCredSegmentTable.

For credential type where the disclosure of the credential would compromise the credential (e.g. shared secrets), when this object is accessed for reading, it MUST return a null length (0 length) string and MUST NOT return the configured credential."

::= { ipspCredentialEntry 3 }

ipspCredSize OBJECT-TYPE

SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "This value represents the size of the credential.

If this value is greater than 1024, the ipspCreCredential column will return an empty (0 length) string. In this case, the value of the credential must be retrieved from the ipspCredSegmentTable.

For credential type where the disclosure of the credential would compromise the credential (e.g. shared secrets), when this object is accessed for reading, it MUST return a value of 0 and MUST NOT return the size credential."

```
::= { ipspCredentialEntry 4 }
```

```
ipspCredMngName OBJECT-TYPE
```

```
SYNTAX      SnmpAdminString (SIZE(0..32))
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
"This value is used as an index into the  
ipspIpsecCredMngServiceTable. For IDs that have no credential  
management service, this value is left blank."
```

```
::= { ipspCredentialEntry 5 }
```

```
ipspCredRemoteID OBJECT-TYPE
```

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

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

Various Authors

[Page 105]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

```
STATUS      current
```

```
DESCRIPTION
```

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

```
::= { ipspCredentialEntry 6 }
```

```
ipspCredAdminStatus OBJECT-TYPE
```

```
SYNTAX      IpspAdminStatus
```

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

```
STATUS      current
```

```
DESCRIPTION
```

```
"Indicates whether this credential should be considered active.  
Rows with a disabled status must not be used for any purpose,  
including IKE or IPSEC processing."
```

```
For credentials whose size does not exceed the maximum size  
for the ipspCredCredential, it may be set to enabled during  
row creation. For larger credentials, it should be left as  
disabled until all rows have been uploaded to the  
ipspCredSegmentTable."
```

```
DEFVAL { disabled }
```

```
::= { ipspCredentialEntry 7 }
```

```
ipspCredLastChanged OBJECT-TYPE
```


SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The value of sysUpTime when this row was last modified or
 created either through SNMP SETs or by some other external
 means."
 ::= { ipspCredentialEntry 8 }

ipspCredStorageType 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."
DEFVAL { nonVolatile }
 ::= { ipspCredentialEntry 9 }

ipspCredRowStatus OBJECT-TYPE

SYNTAX RowStatus

Various Authors

[Page 106]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

MAX-ACCESS read-create

STATUS current

DESCRIPTION

 "This object indicates the conceptual status of this row.

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

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

::= { ipspCredentialEntry 10 }

--

-- Credential Segment Value Table

--

ipspCredentialSegmentTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpspCredentialSegmentEntry

MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"A table of credential segments. This table is used for
credentials which are larger than the maximum size allowed
for ipspCredCredential."
 ::= { ipspConfigObjects 35 }

ipspCredentialSegmentEntry OBJECT-TYPE
SYNTAX IpspCredentialSegmentEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"A row in the ipspCredentialSegmentTable."
INDEX { ipspCredName, ipspCredSegIndex }
 ::= { ipspCredentialSegmentTable 1 }

IpspCredentialSegmentEntry ::= SEQUENCE {
 ipspCredSegIndex Integer32,
 ipspCredSegValue OCTET STRING,
 ipspCredSegLastChanged TimeStamp,
 ipspCredSegStorageType StorageType,
 ipspCredSegRowStatus RowStatus
}

ipspCredSegIndex OBJECT-TYPE
SYNTAX Integer32 (1..65535)
MAX-ACCESS not-accessible
STATUS current

DESCRIPTION

"This object represents the segment number for this segment.

By default, each segment will be 1024 octets. However, when
this table is accessed using a context of 'ipsp4096',
'ipsp8192' or 'ipsp16384' a segment size of 4096, 8192 or
16384 (respectively) will be used instead.

The number of rows which need to be retrieved or set can be
calculated by obtaining the value of the ipspCredSize column
from the corresponding ipspCredentialTable row and dividing it
by the segment size."

```
::= { ipspCredentialSegmentEntry 1 }
```

ipspCredSegValue OBJECT-TYPE

SYNTAX OCTET STRING

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"This object represents one segment of the credential.

By default, each complete segment will be 1024 octets. (The last row for a given credential might be smaller, if the credential size is not a multiple of the segment size).

An implementation may optionally support segment sizes of 256, 4096, 8192 or the full object size when this table is accessed using a context of 'ipspCred256', 'ipspCred4096', 'ipspCred8192' or 'ipspCredFull' (respectively).

The number of rows which need to be retrieved or set can be calculated by obtaining the value of the ipspCredSize column from the corresponding ipspCredentialTable row and dividing it by the segment size."

```
::= { ipspCredentialSegmentEntry 2 }
```

ipspCredSegLastChanged OBJECT-TYPE

SYNTAX TimeStamp

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of sysUpTime when this credential was last modified or created either through SNMP SETs or by some other external means. Note that the last changed type will be the same for all segments of the credential."

```
::= { ipspCredentialSegmentEntry 3 }
```

ipspCredSegStorageType OBJECT-TYPE

Various Authors

[Page 108]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

SYNTAX StorageType

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The storage type for this row. This object is read-only. Rows

in this table have the same value as the ipspCredStorageType
for the corresponding row in the ipspCredentialTable."
DEFVAL { nonVolatile }
::= { ipspCredentialSegmentEntry 4 }

ipspCredSegRowStatus OBJECT-TYPE

SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION

"This object indicates the conceptual status of this row.

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

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

::= { ipspCredentialSegmentEntry 5 }

--
--
-- Notification objects information
--
--

ipspNotificationVariables OBJECT IDENTIFIER ::= { ipspNotificationObjects 1 }

ipspNotifications OBJECT IDENTIFIER ::= { ipspNotificationObjects 0 }

ipspActionExecuted OBJECT-TYPE

SYNTAX VariablePointer
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION

"Points to the action instance that was executed that
resulted in the notification being sent."

::= { ipspNotificationVariables 1 }

ipspIPInterfaceType OBJECT-TYPE

SYNTAX InetAddressType
MAX-ACCESS accessible-for-notify

```
STATUS      current
DESCRIPTION
    "Contains the interface type for the interface that the
    packet which triggered the notification in question is
    passing through."
::= { ipspNotificationVariables 2 }
```

```
ipspIPInterfaceAddress OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  accessible-for-notify
STATUS      current
DESCRIPTION
    "Contains the interface address for the interface that the
    packet which triggered the notification in question is
    passing through."
::= { ipspNotificationVariables 3 }
```

```
ipspIPSourceType OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS  accessible-for-notify
STATUS      current
DESCRIPTION
    "Contains the source address type of the packet which
    triggered the notification in question."
::= { ipspNotificationVariables 4 }
```

```
ipspIPSourceAddress OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  accessible-for-notify
STATUS      current
DESCRIPTION
    "Contains the source address of the packet which triggered the
    notification in question."
::= { ipspNotificationVariables 5 }
```

```
ipspIPDestinationType OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS  accessible-for-notify
STATUS      current
DESCRIPTION
    "Contains the destination address type of the packet which
    triggered the notification in question."
::= { ipspNotificationVariables 6 }
```

```
ipspIPDestinationAddress OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  accessible-for-notify
STATUS      current
```

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

DESCRIPTION

"Contains the destination address of the packet which triggered the notification in question."

::= { ipspNotificationVariables 7 }

ipspPacketDirection OBJECT-TYPE

SYNTAX INTEGER { inbound(1), outbound(2) }

MAX-ACCESS accessible-for-notify

STATUS current

DESCRIPTION

"Indicates if the packet which triggered the action in question was inbound or outbound."

::= { ipspNotificationVariables 8 }

ipspPacketPart OBJECT-TYPE

SYNTAX OCTET STRING

MAX-ACCESS accessible-for-notify

STATUS current

DESCRIPTION

"Is the front part of the packet that triggered this notification. The size is determined by the value of 'IpspIPPacketLogging' or the size of the packet, whichever is smaller."

::= { ipspNotificationVariables 9 }

ipspActionNotification NOTIFICATION-TYPE

OBJECTS { ipspActionExecuted, ipspIPInterfaceType,
 ipspIPInterfaceAddress,
 ipspIPSourceType, ipspIPSourceAddress,
 ipspIPDestinationType,
 ipspIPDestinationAddress,
 ipspPacketDirection }

STATUS current

DESCRIPTION

"Notification that an action was executed by a rule. Only actions with logging enabled will result in this notification getting sent. The objects sent must include the ipspActionExecuted object which will indicate which action was executed within the scope of the rule. Additionally the ipspIPSourceType, ipspIPSourceAddress, ipspIPDestinationType, and ipspIPDestinationAddress objects must be included to

indicate the packet source and destination of the packet that triggered the action. Finally the ipspIPInterfaceType, ipspIPInterfaceAddress, and ipspPacketDirection objects are included to indicate which interface the action was executed in association with and if the packet was inbound or outbound

through the endpoint.

Note that compound actions with multiple executed subactions may result in multiple notifications being sent from a single rule execution."

::= { ipspNotifications 1 }

ipspPacketNotification NOTIFICATION-TYPE

OBJECTS { ipspActionExecuted, ipspIPInterfaceType,
ipspIPInterfaceAddress,
ipspIPSourceType, ipspIPSourceAddress,
ipspIPDestinationType,
ipspIPDestinationAddress,
ipspPacketDirection,
ipspPacketPart }

STATUS current

DESCRIPTION

"Notification that a packet passed through an SA. Only SA's created by actions with packet logging enabled will result in this notification getting sent. The objects sent must include the ipspActionExecuted which will indicate which action was executed within the scope of the rule. Additionally, the ipspIPSourceType, ipspIPSourceAddress, ipspIPDestinationType, and ipspIPDestinationAddress, objects must be included to indicate the packet source and destination of the packet that triggered the action. The ipspIPInterfaceType, ipspIPInterfaceAddress, and ipspPacketDirection objects are included to indicate which endpoint the packet was associated with. Finally, ipspPacketPart is including for sending a variable sized part of the front of the packet depending on the value of IspspIPPacketLogging."

::= { ipspNotifications 2 }

```
--
--
-- Conformance information
--
--
ipspCompliances OBJECT IDENTIFIER
    ::= { ipspConformanceObjects 1 }
ipspGroups OBJECT IDENTIFIER
    ::= { ipspConformanceObjects 2 }
--
```

Various Authors

[Page 112]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

```
-- Compliance statements
--
--
ipspRuleFilterCompliance MODULE-COMPLIANCE
    STATUS            current
    DESCRIPTION
        "The compliance statement for SNMP entities that include an
          IPsec MIB implementation with Endpoint, Rules, and filters
          support."
    MODULE -- This Module
        MANDATORY-GROUPS { ipspEndpointGroup,
                           ipspGroupContentsGroup,
                           ipspRuleDefinitionGroup,
                           ipspIPHeaderFilterGroup,
                           ipspStaticFilterGroup }

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

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

    GROUP ipspIPOffsetFilterGroup
```


DESCRIPTION

"This group is mandatory for IPsec Policy implementations which support IP Offset filters. In general, this SHOULD be supported by a compliant IPsec Policy implementation."

GROUP ipspTimeFilterGroup

DESCRIPTION

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

GROUP ipspIpsoHeaderFilterGroup

DESCRIPTION

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

GROUP ipspCredentialFilterGroup

DESCRIPTION

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

GROUP ipspPeerIdFilterGroup

DESCRIPTION

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

OBJECT ipspEndGroupRowStatus

SYNTAX RowStatus {
active(1), createAndGo(4), destroy(6)
}

DESCRIPTION

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

OBJECT ipspEndGroupLastChanged

MIN-ACCESS not-accessible

DESCRIPTION

"This object not required for compliance."

OBJECT ipspGroupContComponentType

SYNTAX INTEGER {
rule(2)

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

```
OBJECT      ipspGroupContRowStatus
SYNTAX      RowStatus {
    active(1), createAndGo(4), destroy(6)
}
```

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

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

```
OBJECT      ipspRuleDefRowStatus
SYNTAX      RowStatus {
    active(1), createAndGo(4), destroy(6)
}
```

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

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

```
OBJECT      ipspCompFiltRowStatus
SYNTAX      RowStatus {
    active(1), createAndGo(4), destroy(6)
}
```

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

```
OBJECT      ipspCompFiltLastChanged
```

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

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

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

OBJECT ipspIpHeadFiltIPVersion
SYNTAX InetAddressType {
 ipv4(1), ipv6(2)
 }
DESCRIPTION
 "Only the ipv4 and ipv6 values make sense for this
 object."

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

OBJECT ipspIpHeadFiltLastChanged

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

OBJECT ipspIpOffFiltRowStatus
SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)

```

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

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

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

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

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

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

OBJECT      ipspCmcDistributionPoint
MIN-ACCESS  read-only
DESCRIPTION
    "Only read-only access is required for compliance."

```

OBJECT ipspCmcThisUpdate
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspCmcNextUpdate
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

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

OBJECT ipspCmcStorageType
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspCmcRowStatus
SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }
MIN-ACCESS read-only
DESCRIPTION
 "Support of the values notInService(2), notReady(3),
 and createAndWait(5) is not required. Only read-only
 access is required for compliance."

OBJECT ipspRctRevokedDate
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspRctRevokedReason
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

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

OBJECT ipspRctStorageType
MIN-ACCESS read-only
DESCRIPTION

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

"Only read-only access is required for compliance."

OBJECT ipspRctRowStatus
SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }
MIN-ACCESS read-only
DESCRIPTION
 "Support of the values notInService(2), notReady(3),
 and createAndWait(5) is not required. Only read-only
 access is required for compliance."

OBJECT ipspIcmsDistinguishedName
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspIcmsPolicyStatement
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspIcmsMaxChainLength
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspIcmsCredentialName
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

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

OBJECT ipspIcmsStorageType
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspIcmsRowStatus

```
SYNTAX      RowStatus {
              active(1), createAndGo(4), destroy(6)
            }
MIN-ACCESS  read-only
DESCRIPTION
```

"Support of the values notInService(2), notReady(3), and createAndWait(5) is not required. Only read-only access is required for compliance."

```
OBJECT      ipspCredType
MIN-ACCESS  read-only
DESCRIPTION
  "Only read-only access is required for compliance."
```

```
OBJECT      ipspCredCredential
MIN-ACCESS  read-only
DESCRIPTION
  "Only read-only access is required for compliance."
```

```
OBJECT      ipspCredMngName
MIN-ACCESS  read-only
DESCRIPTION
  "Only read-only access is required for compliance."
```

```
OBJECT      ipspCredRemoteID
MIN-ACCESS  read-only
DESCRIPTION
  "Only read-only access is required for compliance."
```

```
OBJECT      ipspCredStorageType
MIN-ACCESS  read-only
DESCRIPTION
  "Only read-only access is required for compliance."
```

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

OBJECT ipspCredLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

OBJECT ipspCredFiltRowStatus
SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }
DESCRIPTION

Various Authors

[Page 119]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

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

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

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

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

::= { ipspCompliances 1 }

ipspIPsecCompliance MODULE-COMPLIANCE

STATUS current

DESCRIPTION

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

MODULE -- This Module

```
MANDATORY-GROUPS { ipspIpsecGroup,
                    ipspStaticActionGroup,
                    ipspPreconfiguredGroup }
```

GROUP ipspCompoundActionGroup

DESCRIPTION

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

OBJECT ipspCompActRowStatus

```
SYNTAX RowStatus {
        active(1), createAndGo(4), destroy(6)
```

}

DESCRIPTION

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

OBJECT ipspCompActLastChanged

Various Authors

[Page 120]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

MIN-ACCESS not-accessible

DESCRIPTION

"This object is optional so as not to impose an undue burden on resource-constrained devices."

OBJECT aiipspCompActRowStatus

```
SYNTAX RowStatus {
        active(1), createAndGo(4), destroy(6)
```

}

DESCRIPTION

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

OBJECT aiipspCompActLastChanged

MIN-ACCESS not-accessible

DESCRIPTION

"This object is optional so as not to impose an undue burden on resource-constrained devices."

OBJECT ipspIpsecActRowStatus

```
SYNTAX RowStatus {
        active(1), createAndGo(4), destroy(6)
```

```

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

OBJECT      ipspIpsecActLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is optional so as not to impose an undue
    burden on resource-constrained devices."

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

OBJECT      ipspIpsecPropLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is optional so as not to impose an undue
    burden on resource-constrained devices."

OBJECT      ipspIpsecTranRowStatus

```

```

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

OBJECT      ipspIpsecTranLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is optional so as not to impose an undue
    burden on resource-constrained devices."

OBJECT      ipspSaNegParamRowStatus
SYNTAX      RowStatus {

```

```

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

OBJECT      ipspSaNegParamLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is optional so as not to impose an undue
    burden on resource-constrained devices."

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

OBJECT      ipspAhTranLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is optional so as not to impose an undue
    burden on resource-constrained devices."

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

```

```

OBJECT      ipspEspTranLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is optional so as not to impose an undue
    burden on resource-constrained devices."

OBJECT      ipspIpcompTranRowStatus
SYNTAX      RowStatus {

```

```

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

OBJECT      ipspIpcompTranLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is optional so as not to impose an undue
    burden on resource-constrained devices."

OBJECT      ipspPeerIdAddressType
SYNTAX      InetAddressType {
            ipv4(1), ipv6(2)
        }
DESCRIPTION
    "Only the ipv4 and ipv6 values make sense for this
    object."

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

OBJECT      ipspPeerIdLastChanged
MIN-ACCESS  not-accessible
DESCRIPTION
    "This object is optional so as not to impose an undue
    burden on resource-constrained devices."

OBJECT      ipspCredRowStatus
SYNTAX      RowStatus {
            active(1), createAndGo(4), destroy(6)
        }
DESCRIPTION
    "Support of the values notInService(2), notReady(3),

```

OBJECT ipspCredLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

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

OBJECT ipspCredSegLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

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

OBJECT ipspSaPreActLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

::= { ipspCompliances 2 }

ipspIKECompliance MODULE-COMPLIANCE
 STATUS current
 DESCRIPTION
 "The compliance statement for SNMP entities that include an
 IPsec MIB implementation and supports IKE actions."
 MODULE -- This Module
 MANDATORY-GROUPS { ipspIkeGroup }

 GROUP ipspCompoundActionGroup
 DESCRIPTION

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

OBJECT ipspCompActRowStatus

SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }

DESCRIPTION

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

OBJECT ipspCompActLastChanged

MIN-ACCESS not-accessible

DESCRIPTION

"This object is optional so as not to impose an undue burden on resource-constrained devices."

OBJECT aiipspCompActRowStatus

SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }

DESCRIPTION

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

OBJECT aiipspCompActLastChanged

MIN-ACCESS not-accessible

DESCRIPTION

"This object is optional so as not to impose an undue burden on resource-constrained devices."

OBJECT ipspIkeActRowStatus

SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }

DESCRIPTION

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

OBJECT ipspIkeActLastChanged

MIN-ACCESS not-accessible

DESCRIPTION

"This object is optional so as not to impose an undue burden on resource-constrained devices."

OBJECT ipspIkeActPropRowStatus

SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)

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

OBJECT ipspIkeActPropLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

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

OBJECT ipspIkePropProposalLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

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

OBJECT ipspSaNegParamLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

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

OBJECT ipspIkeIdLastChanged

Various Authors

[Page 126]

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

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

OBJECT ipspPeerIdLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

OBJECT ipspAutoIkeAddressType
SYNTAX InetAddressType {
 ipv4(1), ipv6(2)
 }
DESCRIPTION
 "Only the ipv4 and ipv6 values make sense for this
 object."

OBJECT ipspAutoIkeRowStatus
SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }
DESCRIPTION

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

OBJECT ipspAutoIkeLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue burden on resource-constrained devices."

OBJECT ipspCmcDistributionPoint
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspCmcThisUpdate
MIN-ACCESS read-only

DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspCmcNextUpdate
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

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

OBJECT ipspCmcStorageType
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspCmcRowStatus
SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }
MIN-ACCESS read-only
DESCRIPTION
 "Support of the values notInService(2), notReady(3),

and createAndWait(5) is not required. Only read-only access is required for compliance."

OBJECT ipspRctRevokedDate
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspRctRevokedReason
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

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

OBJECT ipspRctStorageType
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspRctRowStatus
SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }
MIN-ACCESS read-only
DESCRIPTION
 "Support of the values notInService(2), notReady(3),
 and createAndWait(5) is not required. Only read-only
 access is required for compliance."

OBJECT ipspIcmsDistinguishedName
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspIcmsPolicyStatement
MIN-ACCESS read-only
DESCRIPTION

"Only read-only access is required for compliance."

OBJECT ipspIcmsMaxChainLength
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspIcmsCredentialName
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

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

OBJECT ipspIcmsStorageType
MIN-ACCESS read-only
DESCRIPTION
 "Only read-only access is required for compliance."

OBJECT ipspIcmsRowStatus
SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
 }
MIN-ACCESS read-only
DESCRIPTION
 "Support of the values notInService(2), notReady(3),
 and createAndWait(5) is not required. Only read-only

access is required for compliance."

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

OBJECT ipspCredLastChanged

MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

OBJECT ipspCredSegRowStatus
SYNTAX RowStatus {
 active(1), createAndGo(4), destroy(6)
}

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

OBJECT ipspCredSegLastChanged
MIN-ACCESS not-accessible
DESCRIPTION
 "This object is optional so as not to impose an undue
 burden on resource-constrained devices."

::= { ipspCompliances 3 }

ipspLoggingCompliance MODULE-COMPLIANCE

STATUS current

DESCRIPTION

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

MODULE -- This Module

MANDATORY-GROUPS { ipspActionLoggingObjectGroup,
 ipspActionNotificationGroup }

::= { ipspCompliances 4 }

--

--

-- Compliance Groups Definitions

--

Various Authors

[Page 130]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

--

-- Endpoint, Rule, Filter Compliance Groups

--

```

ipspEndpointGroup OBJECT-GROUP
  OBJECTS {
    ipspEndGroupName, ipspEndGroupLastChanged,
    ipspEndGroupStorageType, ipspEndGroupRowStatus
  }
  STATUS current
  DESCRIPTION
    "The IPsec Policy Endpoint Table Group."
  ::= { ipspGroups 1 }

ipspGroupContentsGroup OBJECT-GROUP
  OBJECTS {
    ipspGroupContComponentType, ipspGroupContFilter,
    ipspGroupContComponentName, ipspGroupContLastChanged,
    ipspGroupContStorageType, ipspGroupContRowStatus
  }
  STATUS current
  DESCRIPTION
    "The IPsec Policy Group Contents Table Group."
  ::= { ipspGroups 2 }

ipspIpsecSystemPolicyNameGroup OBJECT-GROUP
  OBJECTS {
    ipspSystemPolicyGroupName
  }
  STATUS current
  DESCRIPTION
    "The System Policy Group Name Group."
  ::= { ipspGroups 3 }

ipspRuleDefinitionGroup OBJECT-GROUP
  OBJECTS {
    ipspRuleDefDescription, ipspRuleDefFilter,
    ipspRuleDefFilterNegated, ipspRuleDefAction,
    ipspRuleDefAdminStatus, ipspRuleDefLastChanged,
    ipspRuleDefStorageType, ipspRuleDefRowStatus
  }
  STATUS current
  DESCRIPTION
    "The IPsec Policy Rule Definition Table Group."
  ::= { ipspGroups 4 }

ipspCompoundFilterGroup OBJECT-GROUP
  OBJECTS {

```

```
        ipspCompFiltDescription, ipspCompFiltLogicType,
        ipspCompFiltLastChanged, ipspCompFiltStorageType,
        ipspCompFiltRowStatus, ipspSubFiltSubfilter,
        ipspSubFiltSubfilterIsNegated, ipspSubFiltLastChanged,
        ipspSubFiltStorageType, ipspSubFiltRowStatus
    }
    STATUS current
    DESCRIPTION
        "The IPsec Policy Compound Filter Table and Filters in
        Compound Filters Table Group."
    ::= { ipspGroups 5 }

ipspStaticFilterGroup OBJECT-GROUP
    OBJECTS { ipspTrueFilter, ipspIkePhase1Filter,
              ipspIkePhase2Filter }
    STATUS current
    DESCRIPTION
        "The static filter group. Currently this is just a true
        filter."
    ::= { ipspGroups 6 }

ipspIPHeaderFilterGroup OBJECT-GROUP
    OBJECTS {
        ipspIpHeadFiltType, ipspIpHeadFiltIPVersion,
        ipspIpHeadFiltSrcAddressBegin, ipspIpHeadFiltSrcAddressEnd,
        ipspIpHeadFiltDstAddressBegin, ipspIpHeadFiltDstAddressEnd,
        ipspIpHeadFiltSrcLowPort, ipspIpHeadFiltSrcHighPort,
        ipspIpHeadFiltDstLowPort, ipspIpHeadFiltDstHighPort,
        ipspIpHeadFiltProtocol, ipspIpHeadFiltIPv6FlowLabel,
        ipspIpHeadFiltLastChanged, ipspIpHeadFiltStorageType,
        ipspIpHeadFiltRowStatus
    }
    STATUS current
    DESCRIPTION
        "The IPsec Policy IP Header Filter Table Group."
    ::= { ipspGroups 7 }

ipspIPOffsetFilterGroup OBJECT-GROUP
    OBJECTS {
        ipspIpOffFiltOffset, ipspIpOffFiltType, ipspIpOffFiltNumber,
        ipspIpOffFiltValue, ipspIpOffFiltLastChanged,
        ipspIpOffFiltStorageType, ipspIpOffFiltRowStatus
    }
    STATUS current
    DESCRIPTION
        "The IPsec Policy IP Offset Filter Table Group."
```

```
::= { ipspGroups 8 }
```

ipspTimeFilterGroup OBJECT-GROUP

```
OBJECTS {
    ipspTimeFiltPeriodStart, ipspTimeFiltPeriodEnd,
    ipspTimeFiltMonthOfYearMask, ipspTimeFiltDayOfMonthMask,
    ipspTimeFiltDayOfWeekMask, ipspTimeFiltTimeOfDayMaskStart,
    ipspTimeFiltTimeOfDayMaskEnd, ipspTimeFiltLastChanged,
    ipspTimeFiltStorageType, ipspTimeFiltRowStatus
}
STATUS current
DESCRIPTION
    "The IPsec Policy Time Filter Table Group."
::= { ipspGroups 9 }
```

ipspIpsoHeaderFilterGroup OBJECT-GROUP

```
OBJECTS {
    ipspIpsoHeadFiltType, ipspIpsoHeadFiltClassification,
    ipspIpsoHeadFiltProtectionAuth, ipspIpsoHeadFiltLastChanged,
    ipspIpsoHeadFiltStorageType, ipspIpsoHeadFiltRowStatus
}
STATUS current
DESCRIPTION
    "The IPsec Policy IPSO Header Filter Table Group."
::= { ipspGroups 10 }
```

ipspCredentialFilterGroup OBJECT-GROUP

```
OBJECTS {
    ipspCredFiltCredentialType, ipspCredFiltMatchFieldName,
    ipspCredFiltMatchFieldValue, ipspCredFiltAcceptCredFrom,
    ipspCredFiltLastChanged, ipspCredFiltStorageType,
    ipspCredFiltRowStatus,

    ipspCmcDistributionPoint, ipspCmcThisUpdate, ipspCmcNextUpdate,
    ipspCmcLastChanged, ipspCmcStorageType, ipspCmcRowStatus,

    ipspRctRevokedDate, ipspRctRevokedReason,
    ipspRctLastChanged, ipspRctStorageType, ipspRctRowStatus,

    ipspIcmsDistinguishedName, ipspIcmsPolicyStatement,
    ipspIcmsMaxChainLength, ipspIcmsCredentialName,
    ipspIcmsLastChanged, ipspIcmsStorageType, ipspIcmsRowStatus,
```

```
    ipspCredType, ipspCredCredential, ipspCredMngName, ipspCredSize,
    ipspCredRemoteID, ipspCredAdminStatus, ipspCredLastChanged,
    ipspCredStorageType, ipspCredRowStatus,

    ipspCredSegValue, ipspCredSegLastChanged,
    ipspCredSegStorageType, ipspCredSegRowStatus
}
```

Various Authors

[Page 133]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

```
STATUS current
DESCRIPTION
    "The IPsec Policy Credential Filter Table Group."
 ::= { ipspGroups 11 }
```

ipspPeerIdFilterGroup OBJECT-GROUP

```
OBJECTS {
    ipspPeerIdFiltIdentityType, ipspPeerIdFiltIdentityValue,
    ipspPeerIdFiltLastChanged, ipspPeerIdFiltStorageType,
    ipspPeerIdFiltRowStatus
}
```

```
STATUS current
DESCRIPTION
    "The IPsec Policy Peer Identity Filter Table Group."
 ::= { ipspGroups 12 }
```

```
--
-- action compliance groups
--
```

ipspCompoundActionGroup OBJECT-GROUP

```
OBJECTS {
    ipspCompActExecutionStrategy, ipspCompActLastChanged,
    ipspCompActStorageType,

    ipspCompActRowStatus, ipspSubActSubActionName,
    aiipspCompActLastChanged, aiipspCompActStorageType,
    aiipspCompActRowStatus
}
```

```
STATUS current
DESCRIPTION
    "The IPsec Policy Compound Action Table and Actions In
    Compound Action Table Group."
```


::= { ipspGroups 13 }

ipspPreconfiguredGroup OBJECT-GROUP

OBJECTS {

ipspSaPreActActionDescription, ipspSaPreActActionLifetimeSec,
ipspSaPreActActionLifetimeKB, ipspSaPreActDoActionLogging,
ipspSaPreActDoPacketLogging, ipspSaPreActDFHandling,
ipspSaPreActActionType, ipspSaPreActAHSPI,
ipspSaPreActAHTransformName, ipspSaPreActAHSharedSecretName,
ipspSaPreActESPSPi, ipspSaPreActESPTransformName,
ipspSaPreActESPEncSecretName, ipspSaPreActESPAuthSecretName,
ipspSaPreActIPCompSPi, ipspSaPreActIPCompTransformName,
ipspSaPreActPeerGatewayIdName, ipspSaPreActLastChanged,
ipspSaPreActStorageType, ipspSaPreActRowStatus,

Various Authors

[Page 134]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

ipspAhTranMaxLifetimeSec, ipspAhTranMaxLifetimeKB,
ipspAhTranAlgorithm, ipspAhTranReplayProtection,
ipspAhTranReplayWindowSize, ipspAhTranLastChanged,
ipspAhTranStorageType,

ipspEspTranMaxLifetimeSec, ipspEspTranMaxLifetimeKB,
ipspEspTranCipherTransformId, ipspEspTranCipherKeyLength,
ipspEspTranCipherKeyRounds, ipspEspTranIntegrityAlgorithmId,
ipspEspTranReplayPrevention, ipspEspTranReplayWindowSize,
ipspEspTranLastChanged, ipspEspTranStorageType,
ipspEspTranRowStatus,

ipspIpcompTranDictionarySize, ipspIpcompTranMaxLifetimeSec,
ipspIpcompTranMaxLifetimeKB, ipspIpcompTranPrivateAlgorithm,
ipspIpcompTranLastChanged, ipspIpcompTranStorageType,
ipspIpcompTranRowStatus,

ipspPeerIdValue, ipspPeerIdType, ipspPeerIdAddress,
ipspPeerIdAddressType, ipspPeerIdCredentialName,
ipspPeerIdLastChanged, ipspPeerIdStorageType,
ipspPeerIdRowStatus,

ipspCredType, ipspCredCredential, ipspCredMngName, ipspCredSize,
ipspCredRemoteID, ipspCredAdminStatus, ipspCredLastChanged,
ipspCredStorageType, ipspCredRowStatus,

```

    ipspCredSegValue, ipspCredSegLastChanged,
    ipspCredSegStorageType, ipspCredSegRowStatus
}
STATUS current
DESCRIPTION
    "This group is the set of objects that support preconfigured
    IPsec actions. These objects are from The Preconfigured
    Action Table. This group also includes objects from the
    shared tables: Peer Identity Table, Credential Table,
    Credential Management Service Table and the AH, ESP, and
    IPComp Transform Tables."
 ::= { ipspGroups 14 }

```

```

ipspStaticActionGroup OBJECT-GROUP
OBJECTS {
    ipspDropAction, ipspAcceptAction, ipspRejectIKEAction,
    ipspDropActionLog, ipspAcceptActionLog, ipspRejectIKEActionLog
}
STATUS current
DESCRIPTION
    "The IPsec Policy Static Actions Group."
 ::= { ipspGroups 15 }

```

```

ipspIpsecGroup OBJECT-GROUP
OBJECTS {
    ipspIpsecActParametersName, ipspIpsecActProposalsName,
    ipspIpsecActUsePfs, ipspIpsecActVendorId, ipspIpsecActGroupId,
    ipspIpsecActPeerGatewayIdName, ipspIpsecActUseIkeGroup,
    ipspIpsecActGranularity, ipspIpsecActMode,
    ipspIpsecActDFHandling, ipspIpsecActDoActionLogging,
    ipspIpsecActDoPacketLogging, ipspIpsecActLastChanged,
    ipspIpsecActStorageType, ipspIpsecActRowStatus,

    ipspIpsecPropTransformsName, ipspIpsecPropLastChanged,
    ipspIpsecPropStorageType, ipspIpsecPropRowStatus,

    ipspIpsecTranTransformName, ipspIpsecTranLastChanged,
    ipspIpsecTranStorageType, ipspIpsecTranRowStatus,

    ipspSaNegParamMinLifetimeSecs, ipspSaNegParamMinLifetimeKB,
    ipspSaNegParamRefreshThreshSecs,
    ipspSaNegParamRefreshThresholdKB,

```

ipspSaNegParamIdleDurationSecs, ipspSaNegParamLastChanged,
ipspSaNegParamStorageType, ipspSaNegParamRowStatus,

ipspAhTranMaxLifetimeSec, ipspAhTranMaxLifetimeKB,
ipspAhTranAlgorithm, ipspAhTranReplayProtection,
ipspAhTranReplayWindowSize, ipspAhTranLastChanged,
ipspAhTranStorageType, ipspAhTranRowStatus,

ipspEspTranMaxLifetimeSec, ipspEspTranMaxLifetimeKB,
ipspEspTranCipherTransformId, ipspEspTranCipherKeyLength,
ipspEspTranCipherKeyRounds, ipspEspTranIntegrityAlgorithmId,
ipspEspTranReplayPrevention, ipspEspTranReplayWindowSize,
ipspEspTranLastChanged, ipspEspTranStorageType,
ipspEspTranRowStatus,

ipspIpcompTranDictionarySize, ipspIpcompTranAlgorithm,
ipspIpcompTranMaxLifetimeSec, ipspIpcompTranMaxLifetimeKB,
ipspIpcompTranPrivateAlgorithm, ipspIpcompTranLastChanged,
ipspIpcompTranStorageType, ipspIpcompTranRowStatus,

ipspPeerIdValue, ipspPeerIdType, ipspPeerIdAddress,
ipspPeerIdAddressType, ipspPeerIdCredentialName,
ipspPeerIdLastChanged, ipspPeerIdStorageType,
ipspPeerIdRowStatus,

ipspCredType, ipspCredCredential, ipspCredMngName, ipspCredSize,
ipspCredRemoteID, ipspCredAdminStatus, ipspCredLastChanged,
ipspCredStorageType, ipspCredRowStatus,

ipspCredSegValue, ipspCredSegLastChanged,
ipspCredSegStorageType, ipspCredSegRowStatus

}

STATUS current

DESCRIPTION

"This group is the set of objects that support IPsec actions. These objects are from The IPsec Policy IPsec Actions Table, The IPsec Proposal Table, and The IPsec Transform Table. This group also includes objects from the shared tables: Peer Identity Table, Credential Table, Negotiation Parameters Table, Credential Management Service Table and the AH, ESP, and IPComp Transform Table."

```
::= { ipspGroups 16 }
```

```
ipspIkeGroup OBJECT-GROUP
```

```
OBJECTS {
```

```
    ipspIkeActParametersName, ipspIkeActThresholdDerivedKeys,  
    ipspIkeActExchangeMode, ipspIkeActAgressiveModeGroupId,  
    ipspIkeActIdentityType, ipspIkeActIdentityContext,  
    ipspIkeActPeerName, ipspIkeActVendorId, ipspIkeActPropName,  
    ipspIkeActDoActionLogging, ipspIkeActDoPacketLogging,  
    ipspIkeActLastChanged, ipspIkeActStorageType,  
    ipspIkeActRowStatus,
```

```
    ipspIkeActPropLastChanged, ipspIkeActPropStorageType,  
    ipspIkeActPropRowStatus,
```

```
    ipspIkePropLifetimeDerivedKeys, ipspIkePropCipherAlgorithm,  
    ipspIkePropCipherKeyLength, ipspIkePropCipherKeyRounds,  
    ipspIkePropHashAlgorithm, ipspIkePropPrfAlgorithm,  
    ipspIkePropVendorId, ipspIkePropDhGroup,  
    ipspIkePropAuthenticationMethod, ipspIkePropMaxLifetimeSecs,  
    ipspIkePropMaxLifetimeKB, ipspIkePropProposalLastChanged,  
    ipspIkePropProposalStorageType, ipspIkePropProposalRowStatus,
```

```
    ipspSaNegParamMinLifetimeSecs, ipspSaNegParamMinLifetimeKB,  
    ipspSaNegParamRefreshThreshSecs,  
    ipspSaNegParamRefreshThresholdKB,  
    ipspSaNegParamIdleDurationSecs, ipspSaNegParamLastChanged,  
    ipspSaNegParamStorageType, ipspSaNegParamRowStatus,
```

```
    ipspIkeIdCredentialName,  
    ipspIkeIdLastChanged, ipspIkeIdStorageType, ipspIkeIdRowStatus,
```

```
    ipspAutoIkeAction, ipspAutoIkeAddressType,  
    ipspAutoIkeSourceAddress, ipspAutoIkeSourcePort,  
    ipspAutoIkeDestAddress, ipspAutoIkeDestPort,  
    ipspAutoIkeProtocol, ipspAutoIkeLastChanged,
```

```
    ipspAutoIkeStorageType, ipspAutoIkeRowStatus,
```

```
    ipspPeerIdValue, ipspPeerIdType, ipspPeerIdAddress,  
    ipspPeerIdAddressType, ipspPeerIdCredentialName,  
    ipspPeerIdLastChanged, ipspPeerIdStorageType,
```

```

    ipspPeerIdRowStatus,

    ipspCmcDistributionPoint, ipspCmcThisUpdate, ipspCmcNextUpdate,
    ipspCmcLastChanged, ipspCmcStorageType, ipspCmcRowStatus,

    ipspRctRevokedDate, ipspRctRevokedReason,
    ipspRctLastChanged, ipspRctStorageType, ipspRctRowStatus,

    ipspIcmsDistinguishedName, ipspIcmsPolicyStatement,
    ipspIcmsMaxChainLength, ipspIcmsCredentialName,
    ipspIcmsLastChanged, ipspIcmsStorageType, ipspIcmsRowStatus,

    ipspCredType, ipspCredCredential, ipspCredMngName, ipspCredSize,
    ipspCredRemoteID, ipspCredAdminStatus, ipspCredLastChanged,
    ipspCredStorageType, ipspCredRowStatus,

    ipspCredSegValue, ipspCredSegLastChanged,
    ipspCredSegStorageType, ipspCredSegRowStatus
}
STATUS current
DESCRIPTION
    "This group is the set of objects that support IKE
    actions.  These objects are from The IPsec Policy IKE Action
    Table, The IKE Action Proposals Table, The IKE Proposal
    Table, The autostart IKE Table and The IKE Identity Table.
    This group also includes objects from the shared tables: Peer
    Identity Table, Credential Management Service Table and
    Negotiation Parameters Table."
 ::= { ipspGroups 17 }

```

```

ipspActionLoggingObjectGroup OBJECT-GROUP
OBJECTS {
    ipspActionExecuted,
    ipspIPInterfaceType,    ipspIPInterfaceAddress,
    ipspIPSourceType,      ipspIPSourceAddress,
    ipspIPDestinationType, ipspIPDestinationAddress,
    ipspPacketDirection,   ipspPacketPart
}
STATUS current
DESCRIPTION
    "Notification objects."
 ::= { ipspGroups 18 }

```

```
ipspActionNotificationGroup NOTIFICATION-GROUP
  NOTIFICATIONS {
    ipspActionNotification,
    ipspPacketNotification
  }
  STATUS current
  DESCRIPTION
    "Notifications."
  ::= { ipspGroups 19 }
```

END

[6.](#) References

[6.1.](#) Normative References

[IPSEC]

Kent, S., and Atkinson, R., "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.

[IKE]

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

[RFC2578]

McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Structure of Management Information Version 2 (SMIV2)", STD 58, [RFC 2578](#), April 1999.

[RFC2579]

McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Textual Conventions for SMIV2", STD 58, [RFC 2579](#), April 1999.

[RFC2580]

McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Conformance Statements for SMIV2", STD 58, [RFC 2580](#), April 1999.

[IPCP]

Jason, J., Rafalow, L., and Vyncke, E., "IPsec Configuration Policy Model", RFCXXX:
[draft-ietf-ipsp-config-policy-model-06.txt](#), August 2002.

[6.2.](#) Informative References

Internet Draft IPsec Policy Configuration MIB module Mar. 2003

[RFC3410]

Case, J., Mundy, R., Partain, D. and B. Stewart,
"Introduction and Applicability Statements for Internet-
Standard Management Framework", [RFC 3410](#), December 2002.

[IPSECPM]

Lortz, V., and Rafalow, L., "IPsec Policy Model White Paper",
November 2000.

[7.](#) 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.

[8.](#) Security Considerations

[8.1.](#) Introduction

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

- 1) To make sure that only the official administrators are allowed

to configure a device, only authenticated administrators should be allowed to do device configuration. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations.

- 2) Unfriendly parties should not be able to read configuration data while the data is in network transit. Any knowledge about a device's IPsec policy configuration could help an unfriendly party compromise that device and/or a network it protects. It is thus important to control even GET access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [\[RFC3410\], section 8](#)), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module, is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

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. 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 initial establishment of IPsec configuration on a device has been achieved, it would be possible to set up IPsec SAs to then also provide

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

8.2. 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

Various Authors

[Page 141]

Internet Draft

IPsec Policy Configuration MIB module

Mar. 2003

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 for authorization control. 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 module will prohibiting them from accessing and/or modifying other sections of the MIB module. 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.

8.3. 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. Aside from those critical parameters, policy administrators have an interest in not divulging any of their policy configuration. Any knowledge about a device's configuration could help an unfriendly party compromise that device. SNMPv3 offers privacy security services, but at the time this

document was written, the only standardized encryption algorithm supported by SNMPv3 is the DES encryption algorithm. Support for other (stronger) cryptographic 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. E.G., it is unwise to configure IPsec parameters implementing 3DES algorithms while only protecting that conversation with single DES.

8.4. 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.

9. Acknowledgments

Many other people contributed thoughts and ideas that influenced this MIB module. Some special thanks are in order the following

Various Authors

[Page 142]

Internet Draft IPsec Policy Configuration MIB module

Mar. 2003

people:

Lindy Foster (Network Associates Laboratories)
John Gillis (ADC)
Jamie Jason (Intel Corporation)
David Partain (Ericsson)
Lee Rafalow (IBM)
Jon Saperia (JDS Consulting)
Eric Vyncke (Cisco Systems)

10. Authors' Addresses

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

Ricky Charlet
Email: rcharlet@alumni.calpoly.edu

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

Robert Story
Revelstone Software
Phone: +1 770 617 3722
Email: rs-snmpr@revelstone.com

Cliff Wang
SmartPipes Inc.
Suite 300, 565 Metro Place South
Dublin, OH 43017
Phone: +1 614 205 0161
E-Mail: cliffwang2000@yahoo.com

[11.](#) Full Copyright Statement

Copyright (C) The Internet Society (2003). 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.