# IPsec Configuration MIB

## draft-ietf-ipsp-ipsec-conf-mib-01.txt

**Wes Hardaker**
**NAI Labs**

## Authors:

**Michael Baer, NAI Labs**
**Ricky Charlet, Redcreek Commincations**
**Wes Hardaker, NAI Labs**
**David Partain, Ericsson**
**Jon Saperia, JDS Consulting**
**Cliff Wang, Smartpipes**

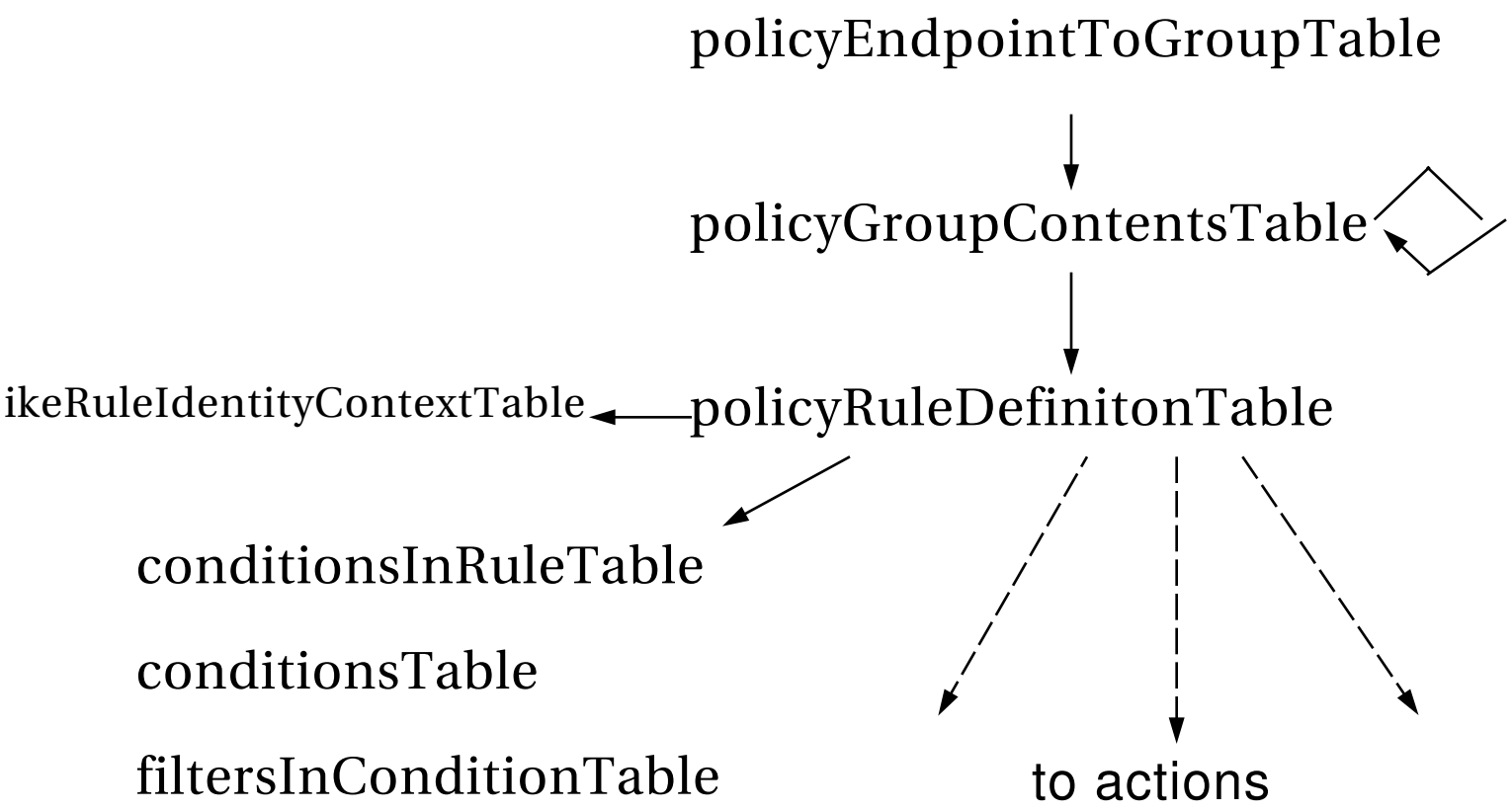
# Overview

- Architecture Overview
- Differences from last time
- Differences from config-policy-model
- To be done
- Discussion
- Questions

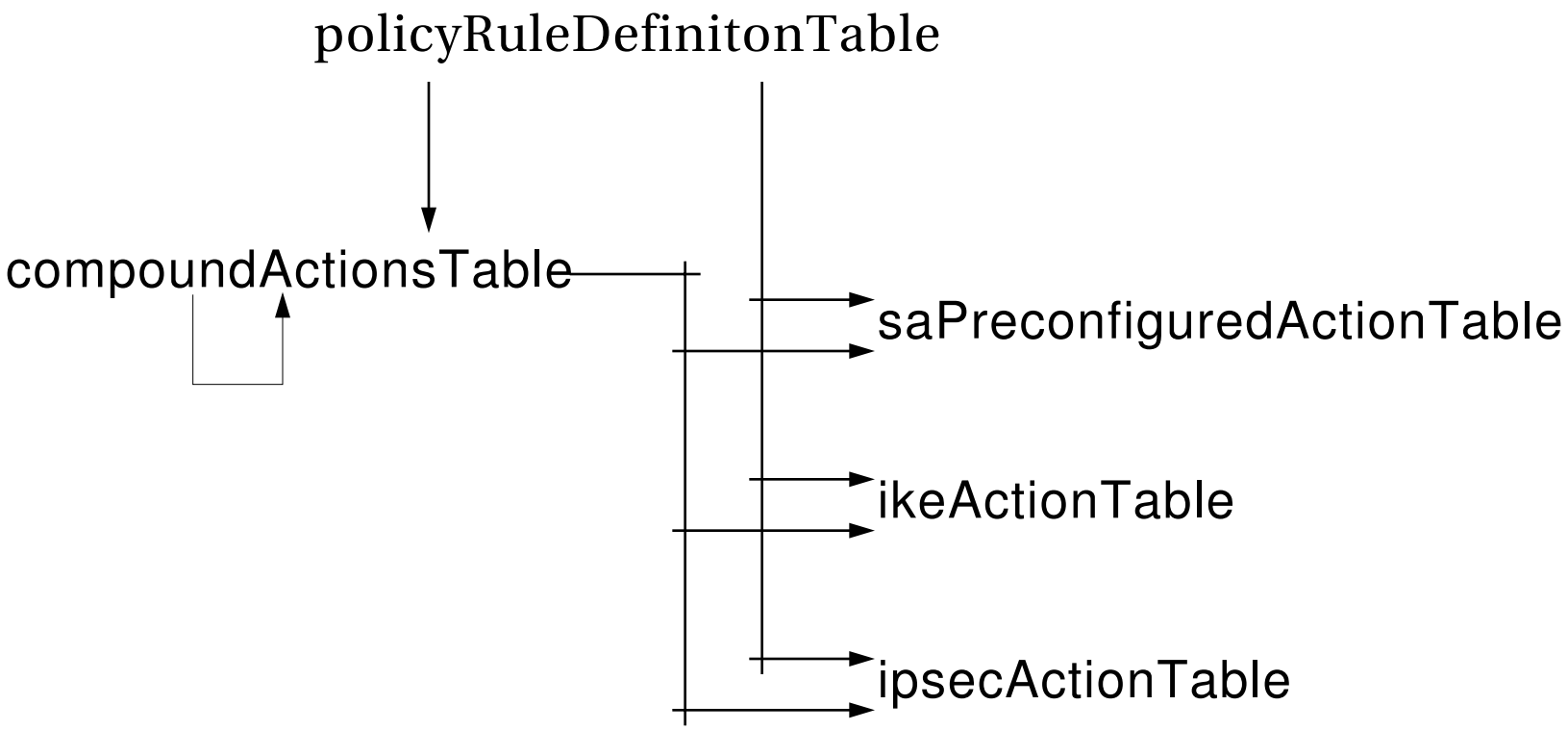
# IPSEC-POLICY-MIB
# Life Signs

- 3645 lines
- 249 Objects
- 23 Tables

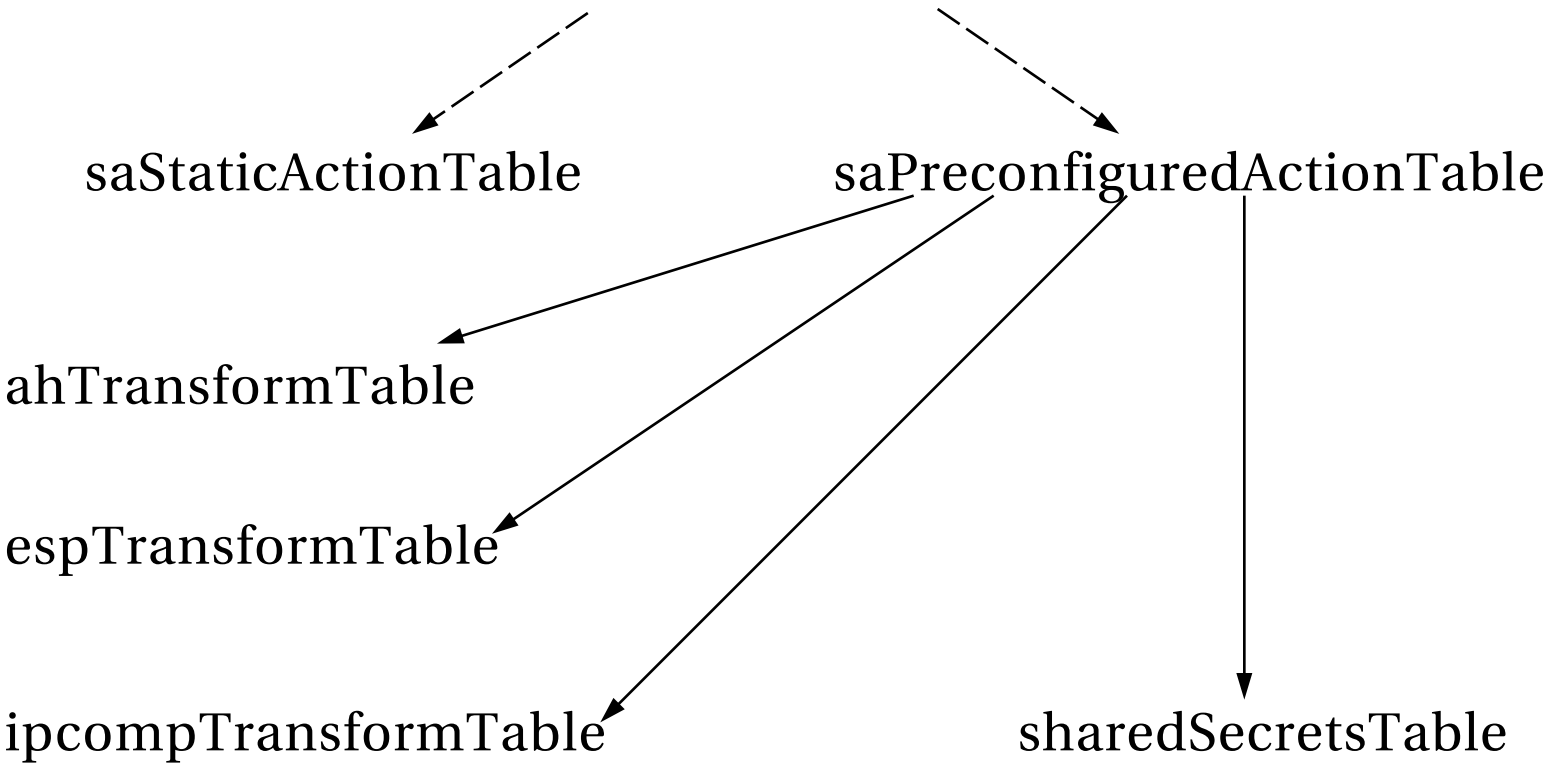
# MIB Tables


policyEndpointToGroupTable
policyGroupContentsTable
ikeRuleIdentityContextTable
policyRuleDefinitonTable
conditionsInRuleTable
conditionsTable
filtersInConditionTable
filterTable
to actions

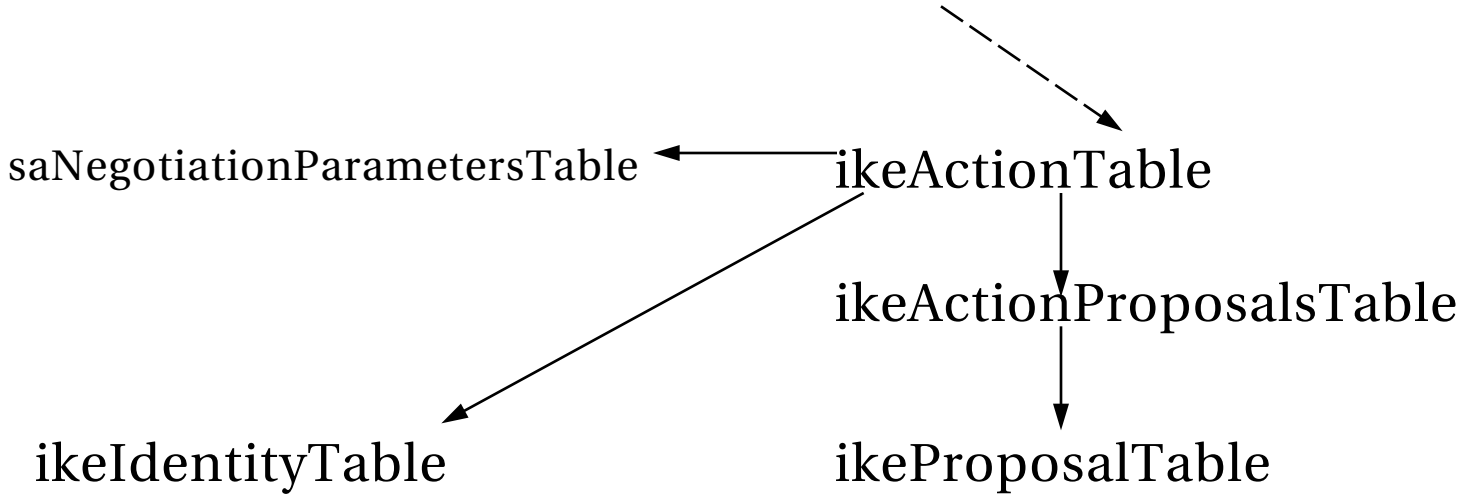
# MIB Tables


policyRuleDefinitonTable
compoundActionsTable
saPreconfiguredActionTable
ikeActionTable
ipsecActionTable

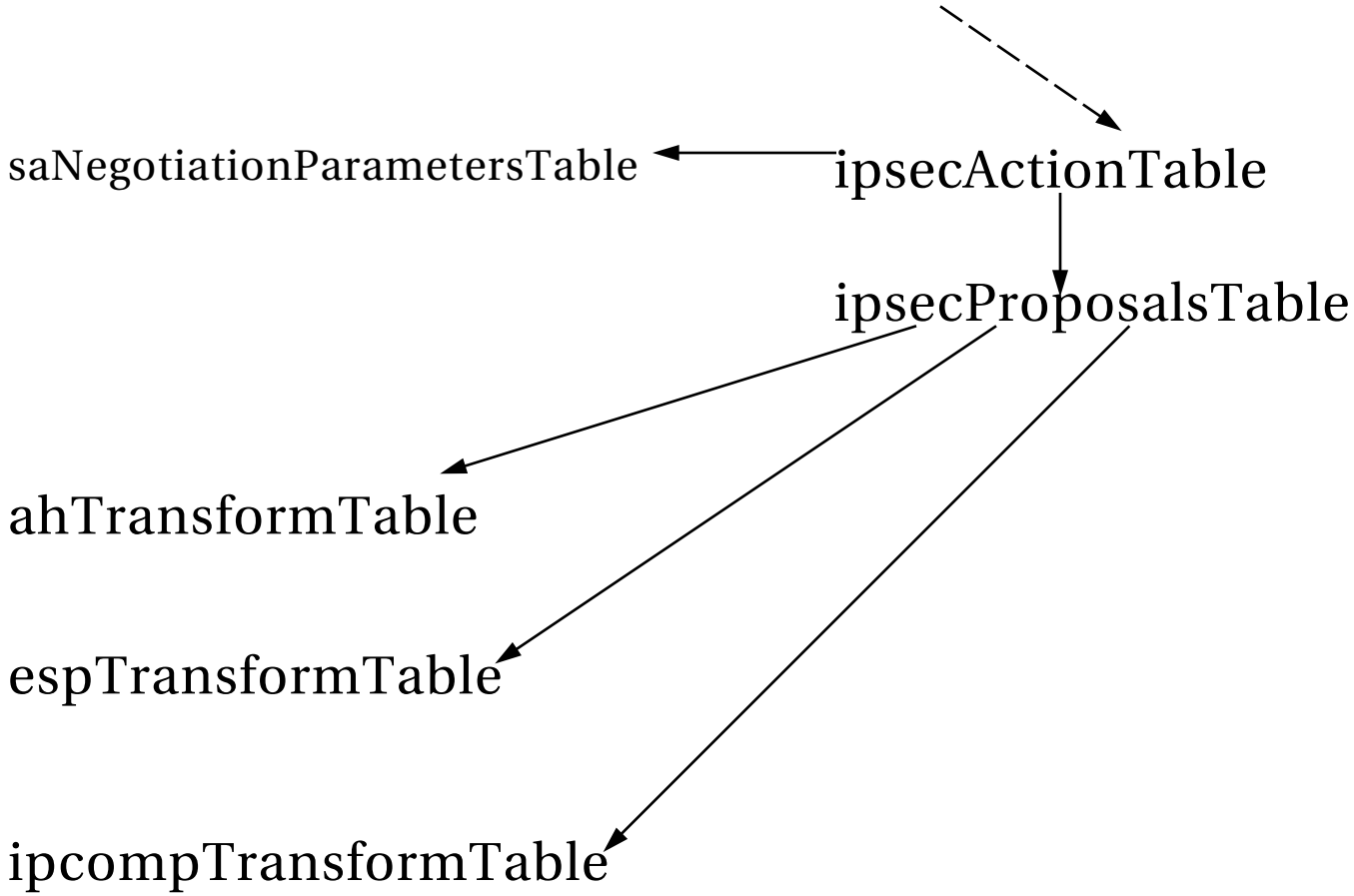
# MIB Tables


saStaticActionTable
saPreconfiguredActionTable
ahTransformTable
espTransformTable
ipcompTransformTable
sharedSecretsTable

# MIB Tables


saNegotiationParametersTable
ikeActionTable
ikeActionProposalsTable
ikeIdentityTable
ikeProposalTable

# MIB Tables


saNegotiationParametersTable
ipsecActionTable
ipsecProposalsTable
ahTransformTable
espTransformTable
ipcompTransformTable

# Differences from last time

- place system policy name into a sub-oid grouping.
- Mention that shared secret keys MUST not be retrievable.
- move to experimental XXX.
- Added global system policy scalar object.
- renumbering of tables.
- blech, bunch o'changes
- make ike proposals definition index derive directly from the
- containmenship table.
- Redo the rule definitions tables.
- Remove ipsecProposalName from ipsecActionTable and add it as a column
- to the ipsecProposalTable and add ipsecActionName as an index to the
- same table.  This allows an action to contain a list of proposals
- which contain a list of transforms.
- minor white space changes.
- ikeActionProposalIndex -> ikeActionProposalPriority
- multiple IKE proposals within a given ikeAction.
- drop saNegotationAction table in favor of pointing directly to the
- ipsecActionTable and ikeActionTable and transforming the
- saNegotationAction into a new saNegotationParametersTable that can be
- referenced by the other two.
- Do group in group functionality via a PolicyGroupContentsTable
- correct oid size problems by decreasing a few sizes on objects in indexes
- add a new revision statement (for friday)
- Reworked the ipsecProposalTable and related transform tables to be a
- list of transforms explicitly listed in the mib rather than a string
- containing a list.
- Minor bug fixes.
- filter table cleanup.  Needs more work (see TODO list).
- Changed aicaPriority to Integer32 from INTEGER.
- remove TDomain/TAddress import from SNMPv2-TC
- implement compound policy actions.
- added new auth-data-len column
- added 7 new columns to saPreconfiguredActionTable:
- LocalSPI, PeerSPI, initialSeqNum, authIV, authIVLength, encIV, & encIVLength
- misc syntax/text fixes, most are minor
- index object filterName should be not-accessable
- Change filterTable to index by a local column and make
- filtersInCondition use that column as an index instead (removing the
- ficFilterName column from that table).
- dfhandling was described wrong in the static action preconfigured table
- entry
- more  static action preconfigured changes, and um, cough, smilint
- checked this time...
- fix some typos to make it pass smilint.
- added saPreconfigured static action table. Still needs compression
- parameters though, but should be ready for AH/ESP use.
- Make SnmpAdminStrings be minimum of 1 in length (now explicit 1..32).
- all lastChanged entries should be read-only, right?
- Redefine the filter table to use the DOI TC's.  Will change again,
- most likely since the data model is likely to change again sligtly.
- change policyEndpointToGroupTable to use IpsecDoiIdentType instead of
- a TDomain/TAddress pairing.
- properly format stuff for inclusion in the draft.
- - minor peGroupPriority rewording.
- - added conditionFilterListType to specify whether filters should be
-  ANDed or ORed.
- - renaming of a few objects which had spelling mistakes and later
-  proved to be duplicates as well.
- last change objects should be read-only, as pointed out by Robert Story.
- Run through smilint and fix numerous problems.
- Remove DHGroupID and use IkeGroupDescription from
  IPSEC-ISAKMP-IKE-DOI-TC.
- minor rewording to endpoint table.
- Many changes from Casey incorporated.

# Differences from last time (Distilled)

- Matches the current model more closely
  - Not complete due to continuing changes to the data model.
- Made use of IPSEC-ISAKMP-IKE-DOI-TC
- Group in group supported.
- Filters can be ANDed or ORed (to support CNF/DNF)
- Preconfigured actions tables
- String lists -> tables (eg list of transforms in a proposal)
- Misc. problems submitted to WG mailing list.

# Differences from data model

- Packet classification is independent of ipsec/QoS/...
  - (Names are generic.  "Rule", "Condition", ...)
- Rule actions specified via RowPointers
  - Allows extensibility and packet classification system to be used by other external action tables (vendor, QoS, ...)
- Filter OO objects combined into one table.
- CNF/DNF implemented in a more flexible way.

# To be done

- Scheduling of policies
- Filter types missing
  - (was almost complete until data model changed)
- Notifications
- Conformance objects

# Discussion

- Lists contained in separate tables
- Too many tables
  - saNegotationParametersTable
    - (lifetime sec/ kb, refresh sec/kb, idle sec)
  - sharedSecretsTable

# Key's table
# vs.
# Keys in each table

Pro's:

- Keys are sent across the wire once.
- Less memory used for large keys.
- Sharing keys across rows/tables easier.

Con's:

- An extra table in an already large MIB.
- Extra step to look up keys associated with a row.

# Implementation Report

- **NAI Labs has implemented the static SA portion of a previous version of the MIB.**

# Contact Info

**Me:** **hardaker@tislabs.com**

**Mailing list:** **ipsec-policy@vpnc.org**