

Internet Engineering Task Force
IPsec Working Group
INTERNET-DRAFT:
Expires in six months

C. Madson, Cisco Systems Inc.
L. Temoshenko, Cisco Systems.
C. Pellecuru, Cisco Systems.
B. Harrison, Tivoli Systems.
S. Ramakrishnan, Cisco Systems.
17 Mar 2003

IPsec Flow Monitoring MIB Textual Conventions
<[draft-ietf-ipsec-flowmon-mib-tc-00.txt](#)>

Status of this Memo

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

This document is a submission to the IETF Internet Protocol Security Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@lists.tislabs.com) or to the editor(s).

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/1id-abstracts.html>

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

To learn the current status of any Internet-Draft, please check the "id- abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on [ftp.is.co.za](ftp://ftp.is.co.za) (Africa), [ftp.nordu.net](ftp://ftp.nordu.net) (Europe), [ftp.munnari.oz.au](ftp://ftp.munnari.oz.au) (Pacific Rim), [ftp.ietf.org](ftp://ftp.ietf.org) (US East Coast), or [ftp.isi.edu](ftp://ftp.isi.edu) (US West Coast).

Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2001-03). All Rights Reserved.

Abstract

This document describes the SMI textual conventions required to support the definition of IPsec MIBs. It is necessary to separate the definition of the textual conventions into a separate document due to their dependence on IANA assigned numbers for transforms and Diffie-Hellman groups supported by IPsec protocol.

Table of Contents

1.	Introduction	3
1.1	Overview	3
1.2	The SNMPv2 Network Management Framework	3
2.	MIB Definitions	4
3.	Intellectual Property	9
4.	Acknowledgements	10
5.	Security Considerations.....	10
6.	IANA Considerations.....	10
7.	Revision History	10
8.	References	10
9.	Editors' Addresses	12
11.	Expiration	13
12.	Full Copyright Statement	13

1. Introduction

1.1. Overview

To support the management needs of IPsec-based networks, we have defined the IPsec Flow Monitor MIB (module IPSEC-FLOW-MONITOR-MIB). The MIB defines a number of objects with enumeration syntax which refer to the numbers assigned by IANA to denote specific elements (e.g.: transforms and Diffie-Hellman groups).

The IANA assigned numbers for ISAKMP and IPsec would continue to evolve as new transforms and Diffie-Hellman groups of standardized. To insulate the definition of the MIB from these changes, it is necessary to define the textual conventions for various types of MIB elements in a separate document.

The purpose of this draft is to define these textual conventions.

Sections [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#) and [11](#) are administrative in nature.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

1.2. The SNMPv2 Network Management Framework

The SNMP Management Framework presently consists of five major components:

- 1) An overall architecture, described in [RFC 2271](#) [[2271](#)].
- 2) Mechanisms for describing and naming objects and events for the purpose of management. The first version of this Structure of Management Information (SMI) is called SMIV1 and described in [RFC 1155](#) [[1155](#)], [RFC 1212](#) [[1212](#)] and [RFC 1215](#) [[1215](#)]. The second version, called SMIV2, is described in [RFC 1902](#) [[1902](#)], [RFC 1903](#) [[1903](#)] and [RFC 1904](#) [[1904](#)].
- 3) Message protocols for transferring management information. The first version of the SNMP message protocol is called SNMPv1 and described in [RFC 1157](#) [[1157](#)]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in [RFC 1901](#) [[1901](#)] and [RFC 1906](#) [[1906](#)]. The third version of the message protocol is called SNMPv3 and described in [RFC 1906](#) [[1906](#)], [RFC 2272](#) [[2272](#)] and [RFC 2274](#) [[2274](#)].

- 4) Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is described in [RFC 1157](#) [[1157](#)]. A second set of protocol operations and associated PDU formats is described in [RFC 1905](#) [[1905](#)].
- 5) A set of fundamental applications described in [RFC 2273](#) [[2273](#)] and the view-based access control mechanism described in [RFC 2275](#) [[2275](#)].

2. MIB Definitions

```
IPSEC-FLOW-MIB-TC DEFINITIONS ::= BEGIN
```

```
IMPORTS
```

```
    experimental,
    MODULE-IDENTITY
-- mib-2
    TEXTUAL-CONVENTION
                                FROM SNMPv2-SMI
                                FROM RFC1213-MIB
                                FROM SNMPv2-TC;
```

```
ipsecFlowMibTC MODULE-IDENTITY
```

```
    LAST-UPDATED "200302171158Z"
```

```
    ORGANIZATION "Tivoli Systems and Cisco Systems"
```

```
    CONTACT-INFO
```

```
        "Tivoli Systems
        Research Triangle Park, NC
```

```

        Cisco Systems
        170 W Tasman Drive
        San Jose, CA 95134
        USA
```

```
        Tel: +1 800 553-NETS
```

```
        E-mail: cs-ipsecmib@external.cisco.com
                 bret_harrison@tivoli.com"
```

```
DESCRIPTION "This MIB module defines the textual conventions
used in the IPsec Flow Monitoring MIB. This includes
Internet DOI numbers defined in RFC 2407, ISAKMP numbers
defined in RFC 2408, and IKE numbers defined in RFC 2409.
```

```

Revision control of this document after publication
will be under the authority of the IANA."
```

```
-- Placeholder anchor
```

```
    ::= { experimental 170 }
```



```
-- ++++++
-- Standard Textual Conventions
-- ++++++
```

ControlProtocol ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

STATUS current

DESCRIPTION

"The protocol used for keying and control. The value of
cp_none indicate manual administration of IPsec tunnels.
This enumeration will be expanded as new keying protocols
are standardized."

SYNTAX INTEGER {

reserved(0),
cpNone(1),
cpIkev1(2),
cpIkev2(3),
cpKink(4),
cpOther(5)

}

Phase1PeerIdentityType ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

STATUS current

DESCRIPTION

"The type of IPsec Phase-1 peer identity.
The peer may be identified by one of the
ID types defined in IPSEC DOI.

id_dn represent the binary DER encoding of the
identity."

SYNTAX INTEGER {

reserved(0),
idIpv4Addr(1),
idFqdn(2),
idDn(3),
idIpv6Addr(4),
idUserFqdn(5),
idIpv4AddrSubnet(6),
idIpv6AddrSubnet(7),
idIpv4AddrRange(8),
idIpv6AddrRange(9),
idDerAsn1Gn(10),
idKeyId(11)


```
}
```

```
IkeNegoMode ::= TEXTUAL-CONVENTION
```

```
    DISPLAY-HINT "d"
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The IPsec Phase-1 IKE negotiation mode."
```

```
    SYNTAX INTEGER {
```

```
        reserved(0),
```

```
        main(1),
```

```
        aggressive(2)
```

```
    }
```

```
IkeHashAlgo  ::= TEXTUAL-CONVENTION
```

```
    DISPLAY-HINT "d"
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The hash algorithm used in IPsec Phase-1  
        IKE negotiations."
```

```
    SYNTAX INTEGER {
```

```
        reserved(0),
```

```
        md5(1),
```

```
        sha(2),
```

```
        tiger(3),
```

```
        sha256(4),
```

```
        sha384(5),
```

```
        sha512(6)
```

```
    }
```

```
IkeAuthMethod ::= TEXTUAL-CONVENTION
```

```
    DISPLAY-HINT "d"
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The authentication method used in IPsec Phase-1 IKE  
        negotiations."
```

```
    SYNTAX INTEGER {
```

```
        reserved(0),
```

```
        preSharedKey(1),
```

```
        dssSignature(2),
```

```
        rsaSignature(3),
```

```
        rsaEncryption(4),
```

```
        revRsaEncryption(5),
```

```
        elGamalEncryption(6),
```

```
        revElGamalEncryption(7),
```

```
        ecsdaSignature(8),
```

```
        gssApiV1(9),
```

```
        gssApiV2(10)
```



```
}
```

```
DiffHellmanGrp ::= TEXTUAL-CONVENTION
```

```
    DISPLAY-HINT "d"
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The Diffie Hellman Group used in negotiations.
```

```
            reserved      -- reserved groups
```

```
            modp768      -- 768-bit MODP
```

```
            modp1024     -- 1024-bit MODP
```

```
            modp1536     -- 1536-bit MODP group
```

```
            ec2nGP155    -- EC2N group on GP[2^155]
```

```
            ec2nGP185    -- EC2N group on GP[2^185]
```

```
            ec2nGF163    -- EC2N group over GF[2^163]
```

```
            ec2nGF283    -- EC2N group over GF[2^283]
```

```
            ec2nGF409    -- EC2N group over GF[2^409]
```

```
            ec2nGF571    -- EC2N group over GF[2^571]
```

```
        "
```

```
    SYNTAX INTEGER {
```

```
        reserved(0),
```

```
        modp768(1),
```

```
        modp1024(2),
```

```
        ec2nGP155(3),
```

```
        ec2nGP185(4),
```

```
        modp1536(5),      -- 1536-bit MODP group
```

```
        ec2nGF163(6),
```

```
        ec2nGF283(8),
```

```
        ec2nGF409(10),
```

```
        ec2nGF571(12)
```

```
    }
```

```
EncapMode ::= TEXTUAL-CONVENTION
```

```
    DISPLAY-HINT "d"
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The encapsulation mode used by an IPsec Phase-2  
        Tunnel."
```

```
    SYNTAX INTEGER{
```

```
        reserved(0),
```

```
        tunnel(1),
```

```
        transport(2)
```

```
    }
```

```
EncryptAlgo ::= TEXTUAL-CONVENTION
```

```
    DISPLAY-HINT "d"
```

```
    STATUS      current
```

```
    DESCRIPTION
```


"The encryption algorithm used in negotiations."

```
SYNTAX INTEGER {  
    reserved(0),  
    espDes(1),  
    esp3des(2),  
    espRc5(3),  
    espIdea(4),  
    espCast(5),  
    espBlowfish(6),  
    esp3idea(7),  
    espRc4(8),  
    espNull(9),  
    espAes(10)  
}
```

Spi ::= TEXTUAL-CONVENTION

DISPLAY-HINT "x"

STATUS current

DESCRIPTION

"The type of the SPI associated with IPsec Phase-2 security associations."

SYNTAX INTEGER (256..4294967295)

AuthAlgo ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

STATUS current

DESCRIPTION

"The authentication algorithm used by a security association of an IPsec Phase-2 Tunnel."

```
SYNTAX INTEGER{  
    reserved(0),  
    hmacMd5(2),  
    hmacSha(3),  
    desMac(4),  
    hmacSha256(5),  
    hmacSha384(6),  
    hmacSha512(7),  
    ripemd(8)  
}
```

CompAlgo ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

STATUS current

DESCRIPTION

"The compression algorithm used by a security association of an IPsec Phase-2 Tunnel."

SYNTAX INTEGER{


```
        reserved(0),
        compOui(1),
        compDeflate(2),
        compLzs(3),
        compLzjh(4)
    }

EndPtType ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
        "The type of identity use to specify an IPsec End Point."
    SYNTAX INTEGER {
        reserved(0),
        idIpv4Addr(1),
        idFqdn(2),
        idUserFqdn(3),
        idIpv4AddrSubnet(4),
        idIpv6Addr(5),
        idIpv6AddrSubnet(6),
        idIpv4AddrRange(7),
        idIpv6AddrRange(8),
        idDerAsn1Dn(9),
        idDerAsn1Gn(10),
        idKeyId(11)
    }

END
```

3. 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.

4. Acknowledgements

The editors would like to thank: Ajay Dankar, Jamal Mohamed, Mayank Jain, Roy Pereira, David McGrew and Lauren Heintz.

5. Security Considerations

Since this MIB defines only textual conventions, there are no security considerations. Security considerations exist only when managed objects are defined with these textual conventions.

6. IANA Considerations

This document is the MIB definitions corresponding to a group of assigned numbers which are maintained by the IANA. The IANA will maintain the MIB in this document as they make new assignments.

This MIB will be maintained in the same manner as the IANAifType-MIB.

7. Revision History

This section will be removed before publication.

Mar 03, 2003. Initial release as [draft-ietf-ipsec-mib-tc-00.txt](#) by separating out the definitions from [draft-ietf-ipsec-flow-monitoring-mib-01.txt](#).

8. References

- [IPDOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", [RFC2407](#), November 1998
- [SECARCH] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", [RFC2401](#), November 1998
- [IKE] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)", [RFC2409](#), November 1998
- [ISAKMP] Maughan, D., Schertler, M., Schneider, M., and Turner, J.,

- "Internet Security Association and Key Management Protocol (ISAKMP)", [RFC2408](#), November 1998
- [1902] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1902](#), January 1996.
- [2271] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", [RFC 2271](#), January 1998
- [1155] Rose, M., and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based Internets", [RFC 1155](#), May 1990
- [1212] Rose, M., and K. McCloghrie, "Concise MIB Definitions", [RFC 1212](#), March 1991
- [1215] M. Rose, "A Convention for Defining Traps for use with the SNMP", [RFC 1215](#), March 1991
- [1903] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1903](#), January 1996.
- [1904] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1904](#), January 1996.
- [1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", [RFC 1157](#), May 1990.
- [1901] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Introduction to Community-based SNMPv2", [RFC 1901](#), January 1996.
- [1906] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1906](#), January 1996.
- [2272] Case, J., Harrington D., Presuhn R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", [RFC 2272](#), January 1998.

- [2274] Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", [RFC 2274](#), January 1998.
- [1905] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1905](#), January 1996.
- [2273] Levi, D., Meyer, P., and B. Stewart, "MPv3 Applications", [RFC 2273](#), SNMP Research, Inc., Secure Computing Corporation, Cisco Systems, January 1998.
- [2275] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", [RFC 2275](#), January 1998.

9. Editor's Addresses

Cheryl Madson
Cisco Systems
170 W Tasman Drive
San Jose, Ca 95134
Phone: +1 (408) 527 2817
EMail: cmadson@cisco.com

Leo Temoshenko
Cisco Systems
170 W Tasman Drive
San Jose, Ca 95134
USA
Phone: +1 (919) 392 8381
EMail: leot@cisco.com

Chinna Narasimha Reddy Pellacuru
Cisco Systems
170 W Tasman Drive
San Jose, Ca 95134
USA
Phone: +1 (408) 527 3109
EMail: pcn@cisco.com

Bret Harrison
Tivoli Systems Inc.
3901 S. Miami Blvd

Durham, NC. 27703
Phone: +1 (919) 224-1000
EMail: bret_harrison@tivoli.com

S Ramakrishnan
Cisco Systems
170 W Tasman Drive
San Jose, Ca 95134
USA
Phone: +1 (408) 527 7309
EMail: rks@cisco.com

10. Expiration

This draft expires Sep 17, 2003.

11. Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.