RFC 9349
Definitions of Managed Objects for IP Traffic Flow Security

Abstract
This document describes managed objects for the management of IP Traffic Flow Security additions to Internet Key Exchange Protocol Version 2 (IKEv2) and IPsec. This document provides a read-only version of the objects defined in the YANG module for the same purpose, which is in "A YANG Data Model for IP Traffic Flow Security" (RFC 9348).

Status of This Memo
This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9349.

Copyright Notice
Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.
1. Introduction

This document defines a Management Information Base (MIB) module for use with network management protocols in the Internet community. IP Traffic Flow Security (IP-TFS) extensions, as defined in [RFC9347], are enhancements to an IPsec tunnel Security Association (SA) to provide improved traffic confidentiality.

The objects defined here are the same as [RFC9348], with the exception that only operational or state data is supported. By making operational data accessible via SNMP, existing network management systems can monitor IP-TFS. This data is listed in the MIB tree in Section 4.1. This module uses the YANG data model as a reference point for managed objects. Note that an IETF MIB model for IPsec was never standardized; however, the structures here could be adapted to existing proprietary MIB implementations where SNMP is used to manage networks.

1.1. 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 [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, [RFC2578], STD 58, [RFC2579] and STD 58, [RFC2580].

2. Terminology and Concepts

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Overview

This document defines the MIB for access to operational parameters of IP Traffic Flow Security (IP-TFS). IP-TFS, defined in [RFC9347], configures a Security Association for tunnel mode IPsec with characteristics that improve traffic confidentiality and reduce bandwidth efficiency loss.

This document is based on the concepts and management model defined in [RFC9348]. This document assumes familiarity with the IPsec concepts described in [RFC4301], IP-TFS as described in [RFC9347], and the IP-TFS management model described in [RFC9348].

This document specifies an extensible operational model for IP-TFS. It reuses the management model defined in [RFC9348]. It allows SNMP systems to read operational objects (which include configured objects) from IP-TFS.

4. Management Objects

4.1. MIB Tree

The following is the MIB registration tree diagram for the IP-TFS extensions.
# IP-TRAFFIC-FLOW-SECURITY-MIB registration tree

```plaintext
--iptfsMIB(1.3.6.1.2.1.500)
  +--iptfsMIBObjects(1)
    |   +--iptfsGroup(1)
    |       +--iptfsConfigTable(1)
    |          +--iptfsConfigTableEntry(1) [iptfsConfigSaIndex]
    |             |   |   |   +-- --- Integer32 iptfsConfigSaIndex(1)
    |             |   |   +-- r-n TruthValue congestionControl(2)
    |             |   |   +-- r-n TruthValue usePathMtuDiscovery(3)
    |             |   |   +-- r-n UnsignedShort outerPacketSize(4)
    |             |   |   +-- r-n CounterBasedGauge64 l2FixedRate(5)
    |             |   |   +-- r-n CounterBasedGauge64 l3FixedRate(6)
    |             |   +-- r-n TruthValue dontFragment(7)
    |             +-- r-n NanoSeconds maxAggregationTime(8)
    +--ipsecStatsGroup(2)
       +--ipsecStatsTable(1)
          +--ipsecStatsTableEntry(1) [ipsecSaIndex]
             |   |   |   |   +-- --- Integer32 ipsecSaIndex(1)
             |   |   +-- r-n Counter64 txPkts(2)
             |   |   +-- r-n Counter64 txOctets(3)
             |   +-- r-n Counter64 txDropPkts(4)
             +-- r-n Counter64 rxPkts(5)
                 +-- r-n Counter64 rxOctets(6)
                 +-- r-n Counter64 rxDropPkts(7)
       +--iptfsInnerStatsGroup(3)
          +--iptfsInnerStatsTable(1)
             +--iptfsInnerStatsTableEntry(1) [iptfsInnerSaIndex]
                |   |   |   |   +-- --- Integer32 iptfsInnerSaIndex(1)
                |   |   +-- r-n Counter64 txInnerPkts(2)
                |   |   +-- r-n Counter64 txInnerOctets(3)
                |   +-- r-n Counter64 rxInnerPkts(4)
                +-- r-n Counter64 rxInnerOctets(5)
                +-- r-n Counter64 rxIncompleteInnerPkts(6)
       +--iptfsOuterStatsGroup(4)
          +--iptfsOuterStatsTable(1)
             +--iptfsOuterStatsTableEntry(1) [iptfsOuterSaIndex]
                |   |   |   |   +-- --- Integer32 iptfsOuterSaIndex(1)
                |   |   +-- r-n Counter64 txExtraPadPkts(2)
                |   |   +-- r-n Counter64 txExtraPadOctets(3)
                |   +-- r-n Counter64 txAllPadPkts(4)
                +-- r-n Counter64 txAllPadOctets(5)
                +-- r-n Counter64 rxExtraPadPkts(6)
                +-- r-n Counter64 rxExtraPadOctets(7)
                +-- r-n Counter64 rxAllPadPkts(8)
                +-- r-n Counter64 rxAllPadOctets(9)
                +-- r-n Counter64 rxErroredPkts(10)
                +-- r-n Counter64 rxMissedPkts(11)
```

---

RFC 9349

Definitions of Managed Objects for IP-TFS

January 2023

Fedyk & Kinzie

Standards Track

Page 4
4.2. SNMP

The following is the MIB for IP-TFS. The congestion control algorithm in [RFC5348] is referenced in the MIB text.

```plaintext
<CODE BEGINS> file "iptfs-mib.mib"

-- *----------------------------------------------------------------
-- *  IP-TRAFFIC-FLOW-SECURITY-MIB Module
-- *----------------------------------------------------------------

IP-TRAFFIC-FLOW-SECURITY-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE,
    Integer32, Unsigned32, Counter64, mib-2
    FROM SNMPv2-SMI
    CounterBasedGauge64
    FROM HCNUM-TC
    MODULE-COMPLIANCE, OBJECT-GROUP
    FROM SNMPv2-CONF
    TEXTUAL-CONVENTION,
    TruthValue
    FROM SNMPv2-TC;

iptfsMIB MODULE-IDENTITY
    LAST-UPDATED "202301310000Z"
    ORGANIZATION "IETF IPsecme Working Group"
    CONTACT-INFO
        "Author: Don Fedyk
         <mailto:dfedyk@labn.net>
         Author: Eric Kinzie
         <mailto:ekinzie@labn.net>
"

DESCRIPTION
    "This module defines the configuration and operational
    state for managing the IP Traffic Flow Security
    functionality (RFC 9349).

    Copyright (c) 2023 IETF Trust and the persons identified
    as authors of the code. All rights reserved.

    Redistribution and use in source and binary forms,
    with or without modification, is permitted pursuant
    to, and subject to the license terms contained in,
    the Simplified BSD License set forth in Section 4.c
    of the IETF Trust's Legal Provisions Relating to IETF

    This version of this SNMP MIB module is part of RFC 9349;
```
see the RFC itself for full legal notices.

REVISION  "202301310000Z"
DESCRIPTION
  "Initial revision. Derived from the IP-TFS YANG
  Data Model."
  ::= { mib-2 246}
--
-- Textual Conventions
--
UnsignedShort ::= TEXTUAL-CONVENTION
  DISPLAY-HINT "d"
  STATUS      current
  DESCRIPTION "xs:unsignedShort"
  SYNTAX      Unsigned32 (0 .. 65535)

NanoSeconds ::= TEXTUAL-CONVENTION
  DISPLAY-HINT "d-6"
  STATUS      current
  DESCRIPTION
    "Represents the time unit value in nanoseconds."
  SYNTAX      Integer32

-- Objects, Notifications & Conformances

  iptfsMIBObjects  OBJECT IDENTIFIER
    ::= { iptfsMIB 1 }
  iptfsMIBConformance OBJECT IDENTIFIER
    ::= { iptfsMIB 2}

--
-- IP-TFS MIB Object Groups
--

  iptfsGroup OBJECT IDENTIFIER
    ::= { iptfsMIBObjects 1 }

  ipsecStatsGroup OBJECT IDENTIFIER
    ::= { iptfsMIBObjects 2 }

  iptfsInnerStatsGroup OBJECT IDENTIFIER
    ::= { iptfsMIBObjects 3 }

  iptfsOuterStatsGroup OBJECT IDENTIFIER
    ::= { iptfsMIBObjects 4 }

  iptfsConfigTable OBJECT-TYPE
    SYNTAX     SEQUENCE OF IptfsConfigTableEntry
    MAX-ACCESS not-accessible
    STATUS      current
    DESCRIPTION
      "The table containing configuration information for
      IP-TFS."
    ::= { iptfsGroup 1 }

  iptfsConfigTableEntry OBJECT-TYPE
SYNTAX     IptfsConfigTableEntry
MAX-ACCESS not-accessible
STATUS      current
DESCRIPTION  "An entry (conceptual row) containing the information on a particular IP-TFS SA."
INDEX       { iptfsConfigSaIndex }
::= { iptfsConfigTable 1 }

IptfsConfigTableEntry ::= SEQUENCE {
    iptfsConfigSaIndex         Integer32,
    -- identifier information
    congestionControl          TruthValue,
    usePathMtuDiscovery        TruthValue,
    outerPacketSize            UnsignedShort,
    l2FixedRate                CounterBasedGauge64,
    l3FixedRate                CounterBasedGauge64,
    dontFragment               TruthValue,
    maxAggregationTime         NanoSeconds,
    windowSize                 UnsignedShort,
    sendImmediately            TruthValue,
    lostPacketTimerInterval    NanoSeconds
}

iptfsConfigSaIndex OBJECT-TYPE
SYNTAX     Integer32 (1..16777215)
MAX-ACCESS not-accessible
STATUS      current
DESCRIPTION  "A unique value, greater than zero, for each SA. It is recommended that values are assigned contiguously, starting from 1. The value for each entry must remain constant at least from one re-initialization of an entity's network management system to the next re-initialization."
::= { iptfsConfigTableEntry 1 }

congestionControl OBJECT-TYPE
SYNTAX     TruthValue
MAX-ACCESS read-only
STATUS      current
DESCRIPTION  "When set to true, the default, this enables the congestion control on-the-wire exchange of data that is required by congestion control algorithms, as defined by RFC 5348. When set to false, IP-TFS sends fixed-sized packets over an IP-TFS tunnel at a constant rate."
::= { iptfsConfigTableEntry 2 }

usePathMtuDiscovery OBJECT-TYPE
SYNTAX     TruthValue
MAX-ACCESS read-only
STATUS      current
DESCRIPTION  "Packet size is either auto-discovered or manually configured. If usePathMtuDiscovery is true, the system
utilizes path-mtu to determine the maximum IP-TFS packet size. If the packet size is explicitly configured, then it will only be adjusted downward if use-path-mtu is set.

```plaintext
::= { iptfsConfigTableEntry 3 }
```

**outerPacketSize**  
SYNTAX UnsignedShort  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION  
"On transmission, the size of the outer encapsulating tunnel packet (i.e., the IP packet containing Encapsulating Security Payload)."

```plaintext
::= { iptfsConfigTableEntry 4 }
```

**l2FixedRate**  
SYNTAX CounterBasedGauge64  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION  
"The IP-TFS bit rate may be specified as a layer 2 wire rate. On transmission, the target bandwidth/bit rate in bits per second (bps) for the IP-TFS tunnel. This rate is the nominal timing for the fixed-size packet. If congestion control is enabled, the rate may be adjusted down."

```plaintext
::= { iptfsConfigTableEntry 5 }
```

**l3FixedRate**  
SYNTAX CounterBasedGauge64  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION  
"The IP-TFS bit rate may be specified as a layer 3 packet rate. On transmission, the target bandwidth/bit rate in bps for the IP-TFS tunnel. This rate is the nominal timing for the fixed-size packet. If congestion control is enabled, the rate may be adjusted down."

```plaintext
::= { iptfsConfigTableEntry 6 }
```

**dontFragment**  
SYNTAX TruthValue  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION  
"On transmission, disable packet fragmentation across consecutive IP-TFS tunnel packets; inner packets larger than what can be transmitted in outer packets will be dropped."

```plaintext
::= { iptfsConfigTableEntry 7 }
```

**maxAggregationTime**  
SYNTAX NanoSeconds  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION  
"On transmission, the maximum aggregation time is the
maximum length of time a received inner packet can be held prior to transmission in the IP-TFS tunnel. Inner packets that would be held longer than this time, based on the current tunnel configuration, will be dropped rather than be queued for transmission.

```plaintext
::= {iptfsConfigTableEntry 8 }
```

`windowSize` OBJECT-TYPE
SYNTAX UnsignedShort
MAX-ACCESS read-only
STATUS current
DESCRIPTION "On reception, the maximum number of out-of-order packets that will be reordered by an IP-TFS receiver while performing the reordering operation. The value 0 disables any reordering."

```plaintext
::= {iptfsConfigTableEntry 9 }
```

`sendImmediately` OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "On reception, send inner packets as soon as possible; do not wait for lost or misordered outer packets. Selecting this option reduces the inner (user) packet delay but can amplify out-of-order delivery of the inner packet stream in the presence of packet aggregation and any reordering."

```plaintext
::= {iptfsConfigTableEntry 10 }
```

`lostPacketTimerInterval` OBJECT-TYPE
SYNTAX NanoSeconds
MAX-ACCESS read-only
STATUS current
DESCRIPTION "On reception, this interval defines the length of time an IP-TFS receiver will wait for a missing packet before considering it lost. If not using send-immediately, then each lost packet will delay inner (user) packets until this timer expires. Setting this value too low can impact reordering and reassembly."

```plaintext
::= {iptfsConfigTableEntry 11 }
```

`ipsecStatsTable` OBJECT-TYPE
SYNTAX SEQUENCE OF IpsecStatsTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "The table containing basic statistics on IPsec."

```plaintext
::= {ipsecStatsGroup 1 }
```

`ipsecStatsTableEntry` OBJECT-TYPE
SYNTAX IpsecStatsTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
An entry (conceptual row) containing the information on a particular IKE SA.

INDEX  { ipsecSaIndex }
::= { ipsecStatsTable 1 }

IpsecStatsTableEntry ::= SEQUENCE {
  ipsecSaIndex               Integer32,
-- packet statistics information
  txPkts                     Counter64,
  txOctets                   Counter64,
  txDropPkts                 Counter64,
  rxPkts                     Counter64,
  rxOctets                   Counter64,
  rxDropPkts                 Counter64
}

ipsecSaIndex OBJECT-TYPE
SYNTAX      Integer32 (1..16777215)
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
  "A unique value, greater than zero, for each SA. It is recommended that values are assigned contiguously, starting from 1. The value for each entry must remain constant at least from one re-initialization of an entity's network management system to the next re-initialization."
::= { ipsecStatsTableEntry 1 }

txPkts OBJECT-TYPE
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
  "Outbound Packet count."
::= { ipsecStatsTableEntry 2 }

taxOctets OBJECT-TYPE
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
  "Outbound Packet bytes."
::= { ipsecStatsTableEntry 3 }

taxDropPkts OBJECT-TYPE
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
  "Outbound dropped packets count."
::= { ipsecStatsTableEntry 4 }

rxPkts OBJECT-TYPE
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS current
DESCRIPTION "Inbound Packet count."
::= { ipsecStatsTableEntry 5 }

rxOctets OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Inbound Packet bytes."
::= { ipsecStatsTableEntry 6 }

rxDropPkts OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Inbound dropped packets."
::= { ipsecStatsTableEntry 7 }

iptfsInnerStatsTable OBJECT-TYPE
SYNTAX SEQUENCE OF IptfsInnerStatsSaEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "The table containing information on IP-TFS inner packets."
::= { iptfsInnerStatsGroup 1 }

iptfsInnerStatsTableEntry OBJECT-TYPE
SYNTAX IptfsInnerStatsSaEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "An entry containing the information on a particular IP-TFS SA."
INDEX { iptfsInnerSaIndex }
::= { iptfsInnerStatsTable 1 }

IptfsInnerStatsSaEntry ::= SEQUENCE {
  iptfsInnerSaIndex          Integer32,
  txInnerPkts                Counter64,
  txInnerOctets              Counter64,
  rxInnerPkts                Counter64,
  rxInnerOctets              Counter64,
  rxIncompleteInnerPkts      Counter64
}

iptfsInnerSaIndex OBJECT-TYPE
SYNTAX Integer32 (1..16777215)
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "A unique value, greater than zero, for each SA. It is recommended that values are assigned contiguously, starting from 1."
The value for each entry must remain constant at least from one re-initialization of an entity's network management system to the next re-initialization.

::= { iptfsInnerStatsTableEntry 1 }

txInnerPkts OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of IP-TFS inner packets sent. This count is whole packets only. A fragmented packet counts as one packet."
::= { iptfsInnerStatsTableEntry 2 }

txInnerOctets OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of IP-TFS inner octets sent. This is inner packet octets only. This does not count padding."
::= { iptfsInnerStatsTableEntry 3 }

rxInnerPkts OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of IP-TFS inner packets received."
::= { iptfsInnerStatsTableEntry 4 }

rxInnerOctets OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of IP-TFS inner octets received. This does not include padding or overhead."
::= { iptfsInnerStatsTableEntry 5 }

rxIncompleteInnerPkts OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of IP-TFS inner packets that were incomplete. Usually, this is due to fragments not received. Also, this may be due to misordering or errors in received outer packets."
::= { iptfsInnerStatsTableEntry 6 }

iptfsOuterStatsTable OBJECT-TYPE
SYNTAX SEQUENCE OF IptfsOuterStatsSaEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
The table containing information on IP-TFS.
::= { iptfsOuterStatsGroup 1 }

iptfsOuterStatsTableEntry OBJECT-TYPE
SYNTAX     IptfsOuterStatsSaEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
 "An entry containing the information on
 a particular IP-TFS SA."
INDEX      { iptfsOuterSaIndex } 
::= { iptfsOuterStatsTable 1 }

IptfsOuterStatsSaEntry ::= SEQUENCE {
  iptfsOuterSaIndex               Integer32,

  -- iptfs packet statistics information
  txExtraPadPkts             Counter64,
  txExtraPadOctets           Counter64,
  txAllPadPkts               Counter64,
  txAllPadOctets             Counter64,
  rxExtraPadPkts             Counter64,
  rxExtraPadOctets           Counter64,
  rxAllPadPkts               Counter64,
  rxAllPadOctets             Counter64,
  rxErroredPkts              Counter64,
  rxMissedPkts               Counter64
}

iptfsOuterSaIndex OBJECT-TYPE
SYNTAX      Integer32 (1..16777215)
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
 "A unique value, greater than zero, for each SA. 
 It is recommended that values are assigned contiguously, 
 starting from 1. 

 The value for each entry must remain constant at least 
 from one re-initialization of an entity's network management 
 system to the next re-initialization."
::= { iptfsOuterStatsTableEntry 1 }

txErroredPkts OBJECT-TYPE
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
 "Total number of transmitted outer IP-TFS packets that 
 included some padding."
::= { iptfsOuterStatsTableEntry 2 }

txMissedPkts OBJECT-TYPE
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION

"Total number of transmitted octets of padding added to outer IP-TFS packets with data."
::= { iptfsOuterStatsTableEntry 3 }

txAllPadPkts OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of transmitted IP-TFS packets that were all padding with no inner packet data."
::= { iptfsOuterStatsTableEntry 4 }

txAllPadOctets OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number transmitted octets of padding added to IP-TFS packets with no inner packet data."
::= { iptfsOuterStatsTableEntry 5 }

rxExtraPadPkts OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of received outer IP-TFS packets that included some padding."
::= { iptfsOuterStatsTableEntry 6 }

rxExtraPadOctets OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of received octets of padding added to outer IP-TFS packets with data."
::= { iptfsOuterStatsTableEntry 7 }

rxAllPadPkts OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of received IP-TFS packets that were all padding with no inner packet data."
::= { iptfsOuterStatsTableEntry 8 }

rxAllPadOctets OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number received octets of padding added to IP-TFS packets with no inner packet data."
::= { iptfsOuterStatsTableEntry 9 }
rxErroredPkts OBJECT-TYPE
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
  "Total number of IP-TFS outer packets dropped due to
  errors."
::= { iptfsOuterStatsTableEntry 10 }

rxMissedPkts OBJECT-TYPE
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
  "Total number of IP-TFS outer packets missing indicated
  by a missing sequence number."
::= { iptfsOuterStatsTableEntry 11 }

--
-- Iptfs Module Compliance
--

iptfsMIBConformances OBJECT IDENTIFIER
  ::= { iptfsMIBConformance 1 }

iptfsMIBGroups OBJECT IDENTIFIER
  ::= { iptfsMIBConformance 2 }

iptfsMIBCompliance MODULE-COMPLIANCE
  STATUS  current
  DESCRIPTION
    "The compliance statement for entities that
    implement the IP-TFS MIB."
  MODULE  -- this module
    MANDATORY-GROUPS {
      iptfsMIBConfGroup,
      ipsecStatsConfGroup,
      iptfsInnerStatsConfGroup,
      iptfsOuterStatsConfGroup
    }

  ::= { iptfsMIBConformances 1 }

--
-- MIB Groups (Units of Conformance)
--

iptfsMIBConfGroup OBJECT-GROUP
  OBJECTS {
    congestionControl,
    usePathMtuDiscovery,
    outerPacketSize,
    l2FixedRate,
    l3FixedRate,
    dontFragment,
    maxAggregationTime,
    windowSize,
    sendImmediately,
lostPacketTimerInterval

}  
STATUS current
DESCRIPTION
"A collection of objects providing per SA IP-TFS configuration."
::= { iptfsMIBGroups 1 }

ipsecStatsConfGroup OBJECT-GROUP
OBJECTS {
  txPkt,  
  txOctets,  
  txDropPkt,  
  rxPkt,  
  rxOctets,  
  rxDropPkt
}
STATUS current
DESCRIPTION
"A collection of objects providing per SA basic statistics."
::= { iptfsMIBGroups 2 }

iptfsInnerStatsConfGroup OBJECT-GROUP
OBJECTS {
  txInnerPkt,  
  txInnerOctets,  
  rxInnerPkt,  
  rxInnerOctets,  
  rxIncompleteInnerPkt
}
STATUS current
DESCRIPTION
"A collection of objects providing per SA IP-TFS inner packet statistics."
::= { iptfsMIBGroups 3 }

iptfsOuterStatsConfGroup OBJECT-GROUP
OBJECTS {
  txExtraPadPkt,  
  txExtraPadOctets,  
  txAllPadPkt,  
  txAllPadOctets,  
  rxExtraPadPkt,  
  rxExtraPadOctets,  
  rxAllPadPkt,  
  rxAllPadOctets,  
  rxErroredPkt,  
  rxMissedPkt
}
STATUS current
DESCRIPTION
"A collection of objects providing per SA IP-TFS outer packet statistics."
::= { iptfsMIBGroups 4 }

END
5. IANA Considerations

The MIB module in this document uses the following IANA-assigned OBJECT IDENTIFIER value, recorded in the "SMI Network Management MGMT Codes Internet-standard MIB" registry:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>246</td>
<td>iptfsMIB</td>
<td>IP-TRAFFIC-FLOW-SECURITY-MIB</td>
</tr>
</tbody>
</table>

Table 1

6. Security Considerations

The MIB specified in this document can read the operational behavior of IP Traffic Flow Security. For the implications regarding write configuration, consult [RFC9347], which defines the functionality.

There are no management objects defined in this MIB module that have a MAX-ACCESS clause of read-write and/or read-create. So, if this MIB module is implemented correctly, then there is no risk that an intruder can alter or create any management objects of this MIB module via direct SNMP SET operations.

Some of the objects in this MIB module may be considered sensitive or vulnerable in some network environments. This includes INDEX objects with a MAX-ACCESS of not-accessible, and any indices from other modules exposed via AUGMENTS. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and objects and their sensitivity/vulnerability:

- iptfsInnerStatsTable and iptfsOuterStatsTable: Access to IP inner and outer Traffic Flow Security statistics can provide information that IP Traffic Flow Security obscures, such as the true activity of the flows using IP Traffic Flow Security.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), there is no control as to who on the secure network is allowed to access and GET (read) the objects in this MIB module.

Implementations SHOULD provide the security features described by the SNMPv3 framework (see [RFC3410]), and implementations claiming compliance to the SNMPv3 standard MUST include full support for authentication and privacy via the User-based Security Model (USM) [RFC3414] with the AES cipher algorithm [RFC3826]. Implementations MAY also provide support for the Transport Security Model (TSM) [RFC5591] in combination with a secure transport such as SSH [RFC5592] or TLS/DTLS [RFC6353].
Further, deployment of SNMP versions prior to SNMPv3 is \textbf{NOT RECOMMENDED}. Instead, it is \textbf{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 \textbf{GET} or \textbf{SET} (change/create/delete) them.

7. References

7.1. Normative References

7.2. Informative References


**Acknowledgements**

The authors would like to thank Chris Hopps, Lou Berger, and Tero Kivinen for their help and feedback on the MIB model.

**Authors' Addresses**

**Don Fedyk**  
LabN Consulting, L.L.C.  
Email: dfedyk@labn.net

**Eric Kinzie**  
LabN Consulting, L.L.C.  
Email: ekinzie@labn.net