

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 22 May 2022

D. Fedyk
E. Kinzie
LabN Consulting, L.L.C.
18 November 2021

Definitions of Managed Objects for IP Traffic Flow Security
draft-ietf-ipsecme-mib-iptfs-03

Abstract

This document describes managed objects for the the management of IP Traffic Flow Security additions to IKEv2 and IPsec. This document provides a read only version of the objects defined in the YANG module for the same purpose.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on 22 May 2022.

Copyright Notice

Copyright (c) 2021 IETFTrust 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.

Internet-Draft

[draft-ietf-ipsecme-mib-iptfs-03](#)

November 2021

Table of Contents

1.	Introduction	2
2.	Terminology & Concepts	3
3.	Overview	3
4.	Management Objects	3
4.1.	MIB Tree	3
4.2.	SNMP	5
5.	IANA Considerations	19
6.	Security Considerations	19
7.	Acknowledgements	20
8.	References	20
8.1.	Normative References	20
8.2.	Informative References	22
	Authors' Addresses	22

[1.](#) Introduction

This document defines a Management Information Base (MIB) module for use with network management protocols in the Internet community. Traffic Flow Security (IP-TFS) extensions as defined in [\[I-D.ietf-ipsecme-iptfs\]](#). IP-TFS provides enhancements to an IPsec tunnel Security Association to provide improved traffic confidentiality.

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, [\[RFC2580\]](#).

The objects defined here are the same as [\[I-D.ietf-ipsecme-yang-iptfs\]](#) with the exception that only operational data is supported. This module uses the YANG model as a reference point for managed objects. Note an IETF MIB model for IPsec was never standardized however the structures here could be adapted to existing MIB implementations.

Internet-Draft

[draft-ietf-ipsecme-mib-iptfs-03](#)

November 2021

[2.](#) Terminology & 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 [\[RFC2119\]](#) [\[RFC8174\]](#) when, and only when, they appear in all capitals, as shown here.

[3.](#) Overview

This document defines configuration and operational parameters of IP traffic flow security (IP-TFS). IP-TFS, defined in [\[I-D.ietf-ipsecme-iptfs\]](#), 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 [\[I-D.ietf-ipsecme-yang-iptfs\]](#). This document assumes familiarity with IP security concepts described in [\[RFC4301\]](#), IP-TFS as described in [\[I-D.ietf-ipsecme-iptfs\]](#) and the IP-TFS management model described in [\[I-D.ietf-ipsecme-yang-iptfs\]](#).

This document specifies an extensible operational model for IP-TFS. It reuses the management model defined in [\[I-D.ietf-ipsecme-yang-iptfs\]](#). It allows SNMP systems to read configured and operational objects of IPTFS.

[4.](#) Management Objects

[4.1.](#) MIB Tree

The following is the MIB registration tree diagram for the IP-TFS extensions.

```
# IETF-IPTFS-MIB registration tree (generated by smidump 0.4.8)
```

```

--iptfsMIB(1.3.6.1.3.500)
+---iptfsMIBObjects(1)
|   +---iptfsGroup(1)
|   |   +---iptfsConfigTable(1)
|   |   |   +---iptfsConfigTableEntry(1) [iptfsConfigSaIndex]
|   |   |   |   +-- --- Integer32      iptfsConfigSaIndex(1)
|   |   |   |   +-- r-n TruthValue    congestionControl(2)
|   |   |   |   +-- r-n TruthValue    usePathMtu(3)
|   |   |   |   +-- r-n UnsignedShort  outerPacketSize(4)
|   |   |   |   +-- r-n Counter64      l2FixedRate(5)
|   |   |   |   +-- r-n Counter64      l3FixedRate(6)
|   |   |   |   +-- r-n TruthValue    dontFragment(7)

```

```

|   |   +-- r-n NanoSeconds    maxAggregationTime(8)
|   |   +-- r-n Unsigned32     windowSize(9)
|   |   +-- r-n TruthValue     sendImmediately(10)
|   |   +-- r-n NanoSeconds    lostPktTimerInt(11)
+---ipsecStatsGroup(2)
|   +---ipsecStatsTable(1)
|   |   +---ipsecStatsTableEntry(1) [ipsecSaIndex]
|   |   |   +-- --- Integer32 ipsecSaIndex(1)
|   |   |   +-- r-n Counter64 txPackets(2)
|   |   |   +-- r-n Counter64 txOctets(3)
|   |   |   +-- r-n Counter64 txDropPackets(4)
|   |   |   +-- r-n Counter64 rxPackets(5)
|   |   |   +-- r-n Counter64 rxOctets(6)
|   |   |   +-- r-n Counter64 rxDropPackets(7)
+---iptfsInnerStatsGroup(3)
|   +---iptfsInnerStatsTable(1)
|   |   +---iptfsInnerStatsTableEntry(1) [iptfsInnerSaIndex]
|   |   |   +-- --- Integer32 iptfsInnerSaIndex(1)
|   |   |   +-- r-n Counter64 txInnerPackets(2)
|   |   |   +-- r-n Counter64 txInnerOctets(3)
|   |   |   +-- r-n Counter64 rxInnerPackets(4)
|   |   |   +-- r-n Counter64 rxInnerOctets(5)
|   |   |   +-- r-n Counter64 rxIncompleteInnerPackets(6)
+---iptfsOuterStatsGroup(4)
|   +---iptfsOuterStatsTable(1)
|   |   +---iptfsOuterStatsTableEntry(1) [iptfsSaIndex]
|   |   |   +-- --- Integer32 iptfsSaIndex(1)
|   |   |   +-- r-n Counter64 txExtraPadPackets(2)
|   |   |   +-- r-n Counter64 txExtraPadOctets(3)

```

```

|         +-- r-n Counter64 txAllPadPackets(4)
|         +-- r-n Counter64 txAllPadOctets(5)
|         +-- r-n Counter64 rxExtraPadPackets(6)
|         +-- r-n Counter64 rxExtraPadOctets(7)
|         +-- r-n Counter64 rxAllPadPackets(8)
|         +-- r-n Counter64 rxAllPadOctets(9)
|         +-- r-n Counter64 rxErroredPackets(10)
|         +-- r-n Counter64 rxMissedPackets(11)
+--iptfsMIBConformance(2)
  +---iptfsMIBConformances(1)
  |   +---iptfsMIBCompliance(1)
  +---iptfsMIBGroups(2)
    +---iptfsMIBConfGroup(1)
    +---ipsecStatsConfGroup(2)
    +---iptfsInnerStatsConfGroup(3)
    +---iptfsOuterStatsConfGroup(4)

```

[4.2.](#) SNMP

The following is the MIB for IP-TFS. The Congestion control algorithm in [[RFC5348](#)] is referenced in the MIB text.

```

-- *-----
-- *
-- *-----

```

```

IETF-IPTFS-MIB DEFINITIONS ::= BEGIN
  IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE,
    Integer32, Unsigned32, Counter64, experimental
    FROM SNMPv2-SMI
    MODULE-COMPLIANCE, OBJECT-GROUP
    FROM SNMPv2-CONF
    TEXTUAL-CONVENTION,
    TruthValue
    FROM SNMPv2-TC;

  iptfsMIB MODULE-IDENTITY
    LAST-UPDATED "202111180000Z"

```

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 XXXX]. Copyright (c) 2021 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 Documents (<https://trustee.ietf.org/license-info>).

This version of this SNMP MIB module is part of RFC XXXX (<https://tools.ietf.org/html/rfcXXXX>); see the RFC

Fedyk & Kinzie

Expires 22 May 2022

[Page 5]

Internet-Draft

[draft-ietf-ipsecme-mib-iptfs-03](#)

November 2021

itself for full legal notices."

REVISION "202111180000Z"

DESCRIPTION

"Initial revision. Derived from the IPTFS Yang Model."

::= { experimental 500 }

--

-- Textual Conventions

--

UnsignedShort ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

STATUS current

DESCRIPTION "xs:unsignedShort"

SYNTAX Unsigned32 (0 .. 65535)

NanoSeconds ::= TEXTUAL-CONVENTION
DISPLAY-HINT "d"
STATUS current
DESCRIPTION
"Represents time unit value in nanoseconds."
SYNTAX Counter64

-- Objects, Notifications & Conformances

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

--

-- IPTFS 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
IPTFS."
::= { iptfsGroup 1 }

```

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

```

```

IptfsConfigTableEntry ::= SEQUENCE {
    iptfsConfigSaIndex      Integer32,

    -- identifier information
    congestionControl        TruthValue,
    usePathMtu               TruthValue,
    outerPacketSize         UnsignedShort,
    l2FixedRate              Counter64,
    l3FixedRate              Counter64,
    dontFragment             TruthValue,
    maxAggregationTime      NanoSeconds,
    windowSize               Unsigned32,
    sendImmediately         TruthValue,
    lostPktTimerInt         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 entity's network management
        system to the next re-initialization."
    ::= { iptfsConfigTableEntry 1 }

```


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."
DEFVAL { false }
::= { iptfsConfigTableEntry 2 }

usePathMtu OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Packet size is either auto-discovered or manually configured. If usePathMtu is true the system utilizes path-mtu to determine maximum IPTFS packet size. If the packet size is explicitly configured then it will only be adjusted downward if use-path-mtu is set."
::= { iptfsConfigTableEntry 3 }

outerPacketSize OBJECT-TYPE
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 the ESP payload)."
::= { iptfsConfigTableEntry 4 }

l2FixedRate OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"TFS bit rate may be specified at layer 2 wire rate. On transmission, target bandwidth/bit rate in bps for iptfs tunnel. This rate is the nominal timing for the fixed size packet. If congestion control is enabled the rate may be adjusted down (or up if unset)."
::= { iptfsConfigTableEntry 5 }

l3FixedRate OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"TFS bit rate may be specified at layer 3 packet rate. On Transmission, target bandwidth/bit rate in bps for iptfs tunnel. This rate is the nominal timing for the fixed size packet. If congestion control is enabled the rate may be adjusted down (or up if unset)."

::= { iptfsConfigTableEntry 6 }

dontFragment OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"On transmission, disable packet fragmentation across consecutive iptfs tunnel packets; inner packets larger than what can be transmitted in outer packets will be dropped."

::= { iptfsConfigTableEntry 7 }

maxAggregationTime OBJECT-TYPE

SYNTAX NanoSeconds

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"On transmission, maximum aggregation time is the maximum length of time a received inner packet can be held prior to transmission in the iptfs 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."

::= { iptfsConfigTableEntry 8 }

windowSize OBJECT-TYPE

SYNTAX Unsigned32(0..65535)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"On reception, the maximum number of out-of-order packets that will be reordered by an iptfs receiver while performing the reordering operation. The value 0 disables any reordering."

::= { 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."

::= { iptfsConfigTableEntry 10 }

lostPktTimerInt OBJECT-TYPE

SYNTAX NanoSeconds

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"On reception, this interval defines the length of time an iptfs 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."

::= { iptfsConfigTableEntry 11 }

ipsecStatsTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpsecStatsTableEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The table containing basic statistics on IPsec."

::= { 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
    txPackets            Counter64,
    txOctets             Counter64,
```

```
    txDropPackets       Counter64,
    rxPackets           Counter64,
    rxOctets            Counter64,
    rxDropPackets       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 entity's network management
system to the next re-initialization."

::= { ipsecStatsTableEntry 1 }

txPackets OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Outbound Packet count."

::= { ipsecStatsTableEntry 2 }

txOctets OBJECT-TYPE

SYNTAX Counter64

MAX-ACCESS read-only

STATUS current
DESCRIPTION
"Outbound Packet bytes."
::= { ipsecStatsTableEntry 3 }

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

rxPackets 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 }

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

iptfsInnerStatsTable OBJECT-TYPE
SYNTAX SEQUENCE OF IptfsInnerSaEntry
MAX-ACCESS not-accessible
STATUS current

DESCRIPTION

"The table containing information on IPTFS Inner Packets."

::= { iptfsInnerStatsGroup 1 }

iptfsInnerStatsTableEntry OBJECT-TYPE

SYNTAX IptfsInnerSaEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An entry containing the information on a particular tfs SA."

INDEX { iptfsInnerSaIndex }

::= { iptfsInnerStatsTable 1 }

IptfsInnerSaEntry ::= SEQUENCE {

iptfsInnerSaIndex Integer32,

txInnerPackets Counter64,

txInnerOctets Counter64,

rxInnerPackets Counter64,

rxInnerOctets Counter64,

rxIncompleteInnerPackets 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 entity's network management system to the next re-initialization."

::= { iptfsInnerStatsTableEntry 1 }

txInnerPackets 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. Does not count padding."
::= { iptfsInnerStatsTableEntry 3 }

rxInnerPackets 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. Does not include padding or overhead."
::= { iptfsInnerStatsTableEntry 5 }

rxIncompleteInnerPackets 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 IptfsOuterSaEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The table containing information on IPTFS."
 ::= { iptfsOuterStatsGroup 1 }

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

IptfsOuterSaEntry ::= SEQUENCE {
iptfsSaIndex Integer32,

-- iptfs packet statistics information
txExtraPadPackets Counter64,
txExtraPadOctets Counter64,
txAllPadPackets Counter64,
txAllPadOctets Counter64,
rxExtraPadPackets Counter64,
rxExtraPadOctets Counter64,
rxAllPadPackets Counter64,
rxAllPadOctets Counter64,
rxErroredPackets Counter64,
rxMissedPackets Counter64
}

iptfsSaIndex 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 entity's network management system to the next re-initialization."

::= { iptfsOuterStatsTableEntry 1 }

txExtraPadPackets 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 }

txExtraPadOctets 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 }

txAllPadPackets 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 }
```

```
rxExtraPadPackets 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 }
```

```
rxAllPadPackets 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 }
```

```
rxErroredPackets OBJECT-TYPE
```

```
SYNTAX Counter64
```

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

```
STATUS current
```

```
DESCRIPTION
```

```
"Total number of IP-TFS outer packets dropped due to  
errors."
```

```
::= { iptfsOuterStatsTableEntry 10 }
```

Internet-Draft

[draft-ietf-ipsecme-mib-iptfs-03](#)

November 2021

```
SYNTAX      Counter64
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "Total number of IP-TFS outer packets missing indicated
    by 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 which
        implement the IPTFS MIB"
    MODULE      -- this module
        MANDATORY-GROUPS {
            iptfsMIBConfGroup,
            ipsecStatsConfGroup,
            iptfsInnerStatsConfGroup,
            iptfsOuterStatsConfGroup
        }

    ::= { iptfsMIBConformances 1 }
```

```
--
```

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

```
--
```

```
iptfsMIBConfGroup OBJECT-GROUP
    OBJECTS {
        congestionControl,
```

```
usePathMtu,  
outerPacketSize ,  
l2FixedRate ,  
l3FixedRate ,  
dontFragment,  
maxAggregationTime,  
windowSize,  
sendImmediately,
```

```
        lostPktTimerInt  
    }  
    STATUS current  
    DESCRIPTION  
        "A collection of objects providing per SA IPTFS  
        Configuration."  
    ::= { iptfsMIBGroups 1 }  
  
ipsecStatsConfGroup OBJECT-GROUP  
    OBJECTS {  
        txPackets,  
        txOctets,  
        txDropPackets,  
        rxPackets,  
        rxOctets,  
        rxDropPackets  
    }  
    STATUS current  
    DESCRIPTION  
        "A collection of objects providing per SA Basic  
        Stats."  
    ::= { iptfsMIBGroups 2 }  
  
iptfsInnerStatsConfGroup OBJECT-GROUP  
    OBJECTS {  
        txInnerPackets,  
        txInnerOctets,  
        rxInnerPackets,  
        rxInnerOctets,  
        rxIncompleteInnerPackets  
    }  
    STATUS current  
    DESCRIPTION
```

```
"A collection of objects providing per SA IPTFS
Inner Packet Statistics."
 ::= { iptfsMIBGroups 3 }
```

```
iptfsOuterStatsConfGroup OBJECT-GROUP
```

```
OBJECTS {
    txExtraPadPackets,
    txExtraPadOctets,
    txAllPadPackets,
    txAllPadOctets,
    rxExtraPadPackets,
    rxExtraPadOctets,
    rxAllPadPackets,
    rxAllPadOctets,
```

Fedyk & Kinzie

Expires 22 May 2022

[Page 18]

Internet-Draft

[draft-ietf-ipsecme-mib-iptfs-03](#)

November 2021

```
        rxErroredPackets,
        rxMissedPackets
    }
STATUS current
DESCRIPTION
    "A collection of objects providing per SA IPTFS
    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 Numbers registry:

Descriptor	OBJECT IDENTIFIER value
iptfs	TBA IANA
ipsec	TBA IANA

6. Security Considerations

The MIB specified in this document can read the operational and configured behavior of IP traffic flow security, for the implications regarding write configuration consult the [[I-D.ietf-ipsecme-iptfs](#)] 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:

- * `iptfsOuterStatsTable` - IPTFS hides the traffic flows through the network, anywhere that access to read SNMP statistics is enabled needs to be protected from third party observation.

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/SET (read/change/create/delete) 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 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.

7. Acknowledgements

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

8. References

8.1. Normative References

[I-D.ietf-ipsecme-iptfs]

Hopps, C., "IP-TFS: Aggregation and Fragmentation Mode for ESP and its Use for IP Traffic Flow Security", Work in Progress, Internet-Draft, [draft-ietf-ipsecme-iptfs-12](https://www.ietf.org/archive/id/draft-ietf-ipsecme-iptfs-12), 8 November 2021, <<https://www.ietf.org/archive/id/draft-ietf-ipsecme-iptfs-12.txt>>.

[I-D.ietf-ipsecme-yang-iptfs]

Fedyk, D. and C. Hopps, "A YANG Data Model for IP Traffic Flow Security", Work in Progress, Internet-Draft, [draft-ietf-ipsecme-yang-iptfs-03](https://www.ietf.org/archive/id/draft-ietf-ipsecme-yang-iptfs-03), 11 November 2021, <<https://www.ietf.org/archive/id/draft-ietf-ipsecme-yang-iptfs-03.txt>>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](https://www.rfc-editor.org/info/rfc2119), [RFC 2119](https://www.rfc-editor.org/info/rfc2119), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

- [RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIV2)", STD 58, [RFC 2578](#), DOI 10.17487/RFC2578, April 1999, <<https://www.rfc-editor.org/info/rfc2578>>.
- [RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIV2", STD 58, [RFC 2579](#), DOI 10.17487/RFC2579, April 1999, <<https://www.rfc-editor.org/info/rfc2579>>.
- [RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", [RFC 3410](#), DOI 10.17487/RFC3410, December 2002, <<https://www.rfc-editor.org/info/rfc3410>>.
- [RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, [RFC 3414](#), DOI 10.17487/RFC3414, December 2002, <<https://www.rfc-editor.org/info/rfc3414>>.
- [RFC3826] Blumenthal, U., Maino, F., and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model", [RFC 3826](#), DOI 10.17487/RFC3826, June 2004, <<https://www.rfc-editor.org/info/rfc3826>>.
- [RFC5591] Harrington, D. and W. Hardaker, "Transport Security Model for the Simple Network Management Protocol (SNMP)", STD 78, [RFC 5591](#), DOI 10.17487/RFC5591, June 2009, <<https://www.rfc-editor.org/info/rfc5591>>.

- [RFC5592] Harrington, D., Salowey, J., and W. Hardaker, "Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)", [RFC 5592](#), DOI 10.17487/RFC5592, June 2009, <<https://www.rfc-editor.org/info/rfc5592>>.

- [RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", STD 78, [RFC 6353](#), DOI 10.17487/RFC6353, July 2011, <<https://www.rfc-editor.org/info/rfc6353>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

8.2. Informative References

- [RFC2580] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Conformance Statements for SMIV2", STD 58, [RFC 2580](#), DOI 10.17487/RFC2580, April 1999, <<https://www.rfc-editor.org/info/rfc2580>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), DOI 10.17487/RFC4301, December 2005, <<https://www.rfc-editor.org/info/rfc4301>>.
- [RFC5348] Floyd, S., Handley, M., Padhye, J., and J. Widmer, "TCP Friendly Rate Control (TFRC): Protocol Specification", [RFC 5348](#), DOI 10.17487/RFC5348, September 2008, <<https://www.rfc-editor.org/info/rfc5348>>.

Authors' Addresses

Don Fedyk
LabN Consulting, L.L.C.

Email: dfedyk@labn.net

Eric Kinzie
LabN Consulting, L.L.C.

Email: ekinzie@labn.net