Internet Engineering Task Force (IETF)
Request for Comments: 9349
Category: Standards Track
ISSN: 2070-1721

D. Fedyk
E. Kinzie
LabN Consulting, L.L.C.

January 2023

Definitions of Managed Objects for IP Traffic Flow Security

Определения управляемых объектов для защиты потоков трафика IP

Аннотация

Этот документ описывает управляемые объекты дополнений защиты потоков трафика IP (IP Traffic Flow Security) для протокола обмена ключами Internet версии 2 (Internet Key Exchange Protocol Version 2 или IKEv2) и IPsec. Документ представляет доступные лишь для чтения версии объектов, определённых в модуле YANG для тех же целей (A YANG Data Model for IP Traffic Flow Security, RFC 9348).

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке https://www.rfc-editor.org/info/rfc9349.

Оглавление

1. Введение

Этот документ определяет модуль MIB (Management Information Base) для использования протоколами сетевого управления в сообществе Internet. Расширения для защиты потоков трафика (IP Traffic Flow Security или IP-TFS), заданные в [RFC9347], расширяют защищённые связи IPsec SA для повышения уровня конфиденциальности трафика.

Определяемые здесь объекты совпадают с заданными в [RFC9348], но поддерживаются лишь данные рабочего состояния. За счёт доступности данных рабочего состояния по протоколу SNMP имеющиеся системы управления сетями могут отслеживать IP-TFS. Эти данные указаны в дереве MIB (параграф 4.1). Модуль использует модель данных YANG в качестве отправной точки. Отметим, что модель IETF MIB для IPsec не была стандартизована, однако приведённые здесь структуры можно адаптировать к имеющимся фирменным реализациям MIB, где для управления сетями применяется SNMP.

1.1. Схема стандартов управления Internet

Подробный обзор документов, описывающих современную схему управления (Internet-Standard Management Framework) приведён в разделе 7 [RFC3410].

Доступ к управляемым объектам происходит через виртуальное хранилище информации, называемое базой управляющей информации (Management Information Base или MIB). Доступ к объектам MIB обычно выполняется по

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

простому протоколу управления сетью (Simple Network Management Protocol или SNMP). Объекты MIB определяются с использованием механизмов, заданных структурой управляющей информации (Structure of Management Information или SMI). Этот документ описывает модуль MIB, соответствующий SMIv2, описанной в STD 58, [RFC2578], [RFC2579] и [RFC2580].

2. Уровни требований

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

3. Обзор

Этот документ задаёт MIB для доступа к рабочим параметрам IP-TFS. Расширение IP-TFS, определённое в [RFC9347], настраивает защищённые свящи (Security Association или SA) для туннельного режима IPsec с характеристиками, повышающими уровень конфиденциальности трафика и сокращающими расход пропускной способности.

Документ основан на концепциях и модели управления [RFC9348]. Предполагается знакомство читателя с концепциями IPsec [RFC4301], IP-TFS [RFC9347] и моделью управления IP-TFS, описанной в [RFC9348].

Документ задаёт расширяемую операционную модель для IP-TFS, используя модель управления из [RFC9348]. Это позволяет системам SNMP читать рабочие объекты (включая настраиваемые) из IP-TFS.

4. Объекты управления

4.1. Дерево MIB

Ниже представлено дерево регистрации MIB для расширений IP-TFS.

```
# дерево регистрации IP-TRAFFIC-FLOW-SECURITY-MIB

--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)
  |  |        +-- r-n UnsignedShort       windowSize(9)
  |  |        +-- r-n TruthValue          sendImmediately(10)
  |  |        +-- r-n NanoSeconds         lostPacketTimerInterval(11)
  |  +--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)
  +--iptfsMIBConformance(2)
     +--iptfsMIBConformances(1)
     |  +--iptfsMIBCompliance(1)
```

```
      +--iptfsMIBGroups(2)
         +--iptfsMIBConfGroup(1)
         +--ipsecStatsConfGroup(2)
         +--iptfsInnerStatsConfGroup(3)
         +--iptfsOuterStatsConfGroup(4)
```

4.2. SNMP

Ниже представлен модуль MIB для IP-TFS. Алгоритм контроля перегрузок [RFC5348] указан в тексте MIB.

```
<CODE BEGINS> file "iptfs-mib.mib"
-- *-------------------------------------------------------------------
-- *  Модуль IP-TRAFFIC-FLOW-SECURITY-MIB
-- *-------------------------------------------------------------------

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
      "Этот модуль задаёт конфигурацию и рабочее состояние для
      управления функциональностью IP-TFS (RFC 9348).

      Авторские права (Copyright (c) 2023) принадлежат IETF Trust и
      лицам, указанным как авторы. Все права защищены.

      Распространение и применение модуля в исходной или двоичной
      форме с изменениями или без таковых разрешено в соответствии с
      лицензией Simplified BSD License, изложенной в параграфе 4.c
      IETF Trust's Legal Provisions Relating to IETF Documents
      (https://trustee.ietf.org/license-info).

      Эта версия модуля SNMP MIB является частью RFC 9349, где
      правовые аспекты приведены более полно.";

    REVISION "202301310000Z"
    DESCRIPTION
            "Исходный выпуск, основанный на модели YANG IP-TFS."
    ::= { mib-2 246}
--
-- Текстовые соглашения
--

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
      "Представляет время в наносекундах."
    SYNTAX      Integer32


-- Объекты, уведомления, соответствия

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

--
-- Группы объектов IP-TFS MIB
```

```
--
   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
               "Таблица конфигурационных данных для IP-TFS."
       ::= { iptfsGroup 1 }

   iptfsConfigTableEntry OBJECT-TYPE
       SYNTAX     IptfsConfigTableEntry
       MAX-ACCESS not-accessible
       STATUS     current
       DESCRIPTION
         "Запись (концептуальная строка) со сведениями об
         отдельной IP-TFS SA."
       INDEX      { iptfsConfigSaIndex }
       ::= { iptfsConfigTable 1 }

  IptfsConfigTableEntry ::= SEQUENCE {
      iptfsConfigSaIndex         Integer32,

   -- Идентификаторы
      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
         "Уникальное значение больше 0 для каждой SA. Рекомендуется
         выделять значения непрерывно, начиная с 1.

         Значение для каждой записи должно сохраняться хотя бы от
         одной инициализации системы сетевого управления объекта
         до другой."
       ::= { iptfsConfigTableEntry 1 }

    congestionControl OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Принятое по умолчанию значение true разрешает обмен
          данными контроля перегрузки по линии, требуемый алгоритмами
          контроля перегрузок, как указано в RFC 5348. При значении
          false IP-TFS передаёт через туннель IP-TFS пакеты
          фиксированного размера с постоянной скоростью."
        ::= { iptfsConfigTableEntry 2 }

    usePathMtuDiscovery OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Размер пакета задаётся вручную или определяется
          автоматически. При usePathMtuDiscovery true система
          использует path-mtu для определения максимального размера
          пакетов IP-TFS. Если размер задан явно, он может лишь
          снижаться при установке use-path-mtu."
        ::= { iptfsConfigTableEntry 3 }

    outerPacketSize OBJECT-TYPE
        SYNTAX      UnsignedShort
```

```
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "При передаче это размер внешнего инкапсулирующего
          туннельного пакета (т. е. пакета IP с ESP)."
        ::= { iptfsConfigTableEntry 4 }

    l2FixedRate OBJECT-TYPE
        SYNTAX      CounterBasedGauge64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Битовая скорость IP-TFS может быть указана как скорость в
          линии L2. При передаче это целевая пропускная способность
          (битовая скорость) в бит/сек (bps) для туннеля IP-TFS. Это
          задаёт номинальную синхронизацию передачи пакетов
          фиксированного размера. При включённом контроле перегрузок
          скорость может снижаться."
        ::= { iptfsConfigTableEntry 5 }

    l3FixedRate OBJECT-TYPE
        SYNTAX      CounterBasedGauge64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Битовая скорость IP-TFS может быть указана как скорость
          пакетов L3. При передаче это целевая пропускная способность
          (битовая скорость) в бит/сек (bps) для туннеля IP-TFS. Это
          задаёт номинальную синхронизацию передачи пакетов
          фиксированного размера. При включённом контроле перегрузок
          скорость может снижаться."
        ::= { iptfsConfigTableEntry 6 }

    dontFragment OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "При передаче запрещает разделять фрагменты пакета по
          разным последовательным пакетам туннеля IP-TFS. Внутренние
          пакеты, размер, не помещающиеся во внешний пакет, будут
          отбрасываться."
        ::= { iptfsConfigTableEntry 7 }

    maxAggregationTime OBJECT-TYPE
        SYNTAX      NanoSeconds
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "При передаче максимальным временем агрегирования является
           наибольшее время удержания вложенных пакетов до отправки в
           туннель IP-TFS. Внутренние пакеты, удерживаемые дольше
           этого времени в текущей конфигурации туннеля будут
           отбрасываться вместо постановки в очередь на передачу."
        ::= { iptfsConfigTableEntry 8 }

    windowSize OBJECT-TYPE
        SYNTAX      UnsignedShort
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "При получении это максимальное число пакетов с нарушением
          порядка, которые будут переупорядочены получателем IP-TFS.
          Значение 0 отключает восстановление порядка."
        ::= { iptfsConfigTableEntry 9 }

    sendImmediately OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "При получении внутренние пакеты передаются как можно
          быстрее без ожидания потерянных и переупорядоченных внешних
          пакетов. Выбор этой опции сокращает задержку вложенных
          (пользовательских) пакетов, но может усилить нарушение
          порядка доставки потока пакетов при наличии агрегирования
          или иного переупорядочения."
        ::= { iptfsConfigTableEntry 10 }

    lostPacketTimerInterval OBJECT-TYPE
        SYNTAX      NanoSeconds
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "При получении этот интервал задаёт время ожидания
          получателем IP-TFS пропущенных пакетов, прежде чем счесть
```

```
            их потерянными. Если не применяется send-immediately,
            каждая потеря будет задерживать внутренние
            (пользовательские) пакеты, пока не завершится отсчёт этого
            таймера. Установка слишком малого значения может влиять на
            переупорядочение и сборку."
          ::= { iptfsConfigTableEntry 11 }

    ipsecStatsTable OBJECT-TYPE
        SYNTAX     SEQUENCE OF IpsecStatsTableEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
          "Таблица базовой статистики IPsec."
        ::= { ipsecStatsGroup 1 }


     ipsecStatsTableEntry OBJECT-TYPE
        SYNTAX     IpsecStatsTableEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
          "Запись (концептуальная строка) со сведения о конкретной
           IKE SA."
        INDEX      { ipsecSaIndex }
        ::= { ipsecStatsTable 1 }

      IpsecStatsTableEntry ::= SEQUENCE {
      ipsecSaIndex               Integer32,
  -- Данные статистики пакетов
      txPkts                     Counter64,
      txOctets                   Counter64,
      txDropPkts                 Counter64,
      rxPkts                     Counter64,
      rxOoctets                  Counter64,
      rxDropPkts                 Counter64
    }

    ipsecSaIndex OBJECT-TYPE
       SYNTAX      Integer32 (1..16777215)
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
         "Уникальное значение больше 0 для каждой SA. Рекомендуется
         выделять значения подряд, начиная с 1. Значение для каждой
         записи должно сохраняться при перезагрузке системы управления
         элемента сети."
       ::= { ipsecStatsTableEntry 1 }


    txPkts OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Счётчик исходящих пакетов."
        ::= { ipsecStatsTableEntry 2 }

    txOctets OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Счётчик байтов в исходящих пакетах."
        ::= { ipsecStatsTableEntry 3 }

    txDropPkts OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Счётчик отброшенных исходящих пакетов."
        ::= { ipsecStatsTableEntry 4 }

    rxPkts OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Счётчик входящих пакетов."
        ::= { ipsecStatsTableEntry 5 }

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

```
        "Счётчик байтов во входящих пакетах."
    ::= { ipsecStatsTableEntry 6 }

rxDropPkts OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
      "Счётчик отброшенных входящих пакетов."
    ::= { ipsecStatsTableEntry 7 }

iptfsInnerStatsTable OBJECT-TYPE
    SYNTAX     SEQUENCE OF IptfsInnerStatsSaEntry
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
      "Таблица сведений о внутренних пакетах IP-TFS."
    ::= { iptfsInnerStatsGroup 1 }

iptfsInnerStatsTableEntry OBJECT-TYPE
   SYNTAX     IptfsInnerStatsSaEntry
   MAX-ACCESS not-accessible
   STATUS     current
   DESCRIPTION
     "Запись со сведения для конкретной 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
     "Уникальное значение больше 0 для каждой SA. Рекомендуется
     выделять значения подряд, начиная с 1. Значение для каждой
     записи должно сохраняться при перезагрузке системы управления
     элемента сети."
   ::= { iptfsInnerStatsTableEntry 1 }

txInnerPkts OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
      "Общее число переданных внутренних пакетов IP-TFS. Считаются
      лишь целые пакеты, т. е. все фрагменты пакета считаются
      одним пакетом."
    ::= { iptfsInnerStatsTableEntry 2 }

txInnerOctets OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
      "Общее число переданных внутренних байтов IP-TFS. Считаются
      только байты внутренних пакетов без учёта заполнения."
    ::= { iptfsInnerStatsTableEntry 3 }

rxInnerPkts OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
      "Общее число полученных внутренних пакетов IP-TFS."
    ::= { iptfsInnerStatsTableEntry 4 }

    rxInnerOctets OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
      "Общее число полученных внутренних байтов IP-TFS. Байты
      заполнения и издержки не учитываются."
    ::= { iptfsInnerStatsTableEntry 5 }

rxIncompleteInnerPkts OBJECT-TYPE
```

```
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Общее число неполных внутренних пакетов IP-TFS. Обычно это
          является результатом отсутствия фрагментов, а также может
          быть следствием нарушения порядка или ошибок в полученных
          внешних пакетах."
      ::= { iptfsInnerStatsTableEntry 6 }

    iptfsOuterStatsTable OBJECT-TYPE
        SYNTAX     SEQUENCE OF IptfsOuterStatsSaEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
          "Таблица со сведениями о IP-TFS."
        ::= { iptfsOuterStatsGroup 1 }

     iptfsOuterStatsTableEntry OBJECT-TYPE
        SYNTAX     IptfsOuterStatsSaEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
          "Запись со сведениями о конкретной IP-TFS SA."
        INDEX      { iptfsOuterSaIndex }
        ::= { iptfsOuterStatsTable 1 }

      IptfsOuterStatsSaEntry ::= SEQUENCE {
      iptfsOuterSaIndex               Integer32,

    -- Статистика для пакетов iptfs
      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
          "Уникальное значение больше 0 для каждой SA. Рекомендуется
          выделять значения подряд, начиная с 1. Значение для каждой
          записи должно сохраняться при перезагрузке системы управления
          элемента сети."
        ::= { iptfsOuterStatsTableEntry 1 }

     txExtraPadPkts OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Число переданных внешних пакетов IP-TFS с заполнением."
        ::= { iptfsOuterStatsTableEntry 2 }

     txExtraPadOctets OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Число октетов заполнения, добавленных во внешние пакеты
          IP-TFS с данными."
        ::= { iptfsOuterStatsTableEntry 3 }

     txAllPadPkts OBJECT-TYPE
        SYNTAX      Counter64
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "Число переданных пакетов IP-TFS, содержащих лишь заполнение
          (без данных во внутренних пакетах)."
        ::= { iptfsOuterStatsTableEntry 4 }

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

```
            "Число переданных октетов заполнения в пакетах IP-TFS без
            данных во внутренних пакетах."
          ::= { iptfsOuterStatsTableEntry 5 }

      rxExtraPadPkts OBJECT-TYPE
          SYNTAX      Counter64
          MAX-ACCESS  read-only
          STATUS      current
          DESCRIPTION
            "Число полученных внешних пакетов IP-TFS с заполнением."
          ::= { iptfsOuterStatsTableEntry 6 }

      rxExtraPadOctets OBJECT-TYPE
          SYNTAX      Counter64
          MAX-ACCESS  read-only
          STATUS      current
          DESCRIPTION
            "Число полученных внешних пакетов IP-TFS с заполнением и
            данными во внутренних пакетах."
          ::= { iptfsOuterStatsTableEntry 7 }

      rxAllPadPkts OBJECT-TYPE
          SYNTAX      Counter64
          MAX-ACCESS  read-only
          STATUS      current
          DESCRIPTION
            "Число полученных внешних пакетов IP-TFS с заполнением
            без внутренних пакетов с данными."
          ::= { iptfsOuterStatsTableEntry 8 }

      rxAllPadOctets OBJECT-TYPE
          SYNTAX      Counter64
          MAX-ACCESS  read-only
          STATUS      current
          DESCRIPTION
            "Число полученных октетов заполнения в пакетах
            IP-TFS без данных во внутренних пакетах."
          ::= { iptfsOuterStatsTableEntry 9 }

      rxErroredPkts OBJECT-TYPE
          SYNTAX      Counter64
          MAX-ACCESS  read-only
          STATUS      current
          DESCRIPTION
            "Число внешних пакетов IP-TFS, отброшенных из-за ошибок."
          ::= { iptfsOuterStatsTableEntry 10 }

      rxMissedPkts OBJECT-TYPE
          SYNTAX      Counter64
          MAX-ACCESS  read-only
          STATUS      current
          DESCRIPTION
            "Число пропущенных внешних пакетов IP-TFS, указанных
            пропусками порядковых номеров."
          ::= { iptfsOuterStatsTableEntry 11 }

  --
  -- Соответствие модуля iptfs
  --

  iptfsMIBConformances OBJECT IDENTIFIER
                       ::= { iptfsMIBConformance 1 }

  iptfsMIBGroups OBJECT IDENTIFIER
                       ::= { iptfsMIBConformance 2 }

  iptfsMIBCompliance MODULE-COMPLIANCE
          STATUS  current
          DESCRIPTION
                  "Заявление о соответствии для объектов,
                  реализующих IP-TFS MIB."
          MODULE  -- this module
                  MANDATORY-GROUPS {
                   iptfsMIBConfGroup,
                   ipsecStatsConfGroup,
                   iptfsInnerStatsConfGroup,
                   iptfsOuterStatsConfGroup
                  }

          ::= { iptfsMIBConformances 1 }

  --
  -- Группы MIB (блоки соответствия)
  --

  iptfsMIBConfGroup OBJECT-GROUP
```

```
        OBJECTS {
                congestionControl,
                usePathMtuDiscovery,
                outerPacketSize ,
                l2FixedRate ,
                l3FixedRate ,
                dontFragment,
                maxAggregationTime,
                windowSize,
                sendImmediately,
                lostPacketTimerInterval
        }
        STATUS  current
        DESCRIPTION
                "Набор объектов, предоставляемых на уровне
                конфигурации IP-TFS SA."
        ::= { iptfsMIBGroups 1 }

ipsecStatsConfGroup OBJECT-GROUP
        OBJECTS {
                txPkts,
                txOctets,
                txDropPkts,
                rxPkts,
                rxOctets,
                rxDropPkts
        }
        STATUS  current
        DESCRIPTION
          "Набор объектов, обеспечивающих базовую статистику по SA."
        ::= { iptfsMIBGroups 2 }

iptfsInnerStatsConfGroup OBJECT-GROUP
        OBJECTS {
                txInnerPkts,
                txInnerOctets,
                rxInnerPkts,
                rxInnerOctets,
                rxIncompleteInnerPkts
        }
        STATUS  current
        DESCRIPTION
          "Набор объектов, обеспечивающих статистику внутренних
          пакетов IP-TFS по SA."
        ::= { iptfsMIBGroups 3 }


iptfsOuterStatsConfGroup OBJECT-GROUP
        OBJECTS {
                txExtraPadPkts,
                txExtraPadOctets,
                txAllPadPkts,
                txAllPadOctets,
                rxExtraPadPkts,
                rxExtraPadOctets,
                rxAllPadPkts,
                rxAllPadOctets,
                rxErroredPkts,
                rxMissedPkts
        }
        STATUS  current
        DESCRIPTION
          "Набор объектов, обеспечивающих статистику внешних
          пакетов IP-TFS по SA."
          "A collection of objects providing per SA IP-TFS
          outer packet statistics."
        ::= { iptfsMIBGroups 4 }

END
<CODE ENDS>
```

5. Взаимодействие с IANA

Описанный здесь модуль MIB использует выделенное IANA значение OBJECT IDENTIFIER, внесенное в реестр SMI Network Management MGMT Codes Internet-standard MIB.

Таблица 1.

Десятичное значение	*Имя*	*Описание*
246	iptfsMIB	IP-TRAFFIC-FLOW-SECURITY-MIB

6. Вопросы безопасности

Описанный здесь модуль MIB может считывать данные рабочего поведения IP-TFS. Последствия этого рассмотрены в [RFC9347], где описана функциональность.

В описанном модуле MIB нет объектов управления с MAX-ACCESS read-write или read-create, поэтому при корректной реализации модуля MIB не возникает риска изменения или создания злоумышленником объектов управления в этом модуле MIB с помощью прямых операций SNMP SET.

Некоторые из объектов модуля MIB могут быть чувствительными или уязвимыми в отдельных сетевых средах. К таким относятся объекты INDEX с MAX-ACCESS not-accessible и другие индексы из других модулей, раскрываемые через AUGMENT. Важно контролировать доступ к этим объектам даже с помощью GET или NOTIFY и может быть даже шифровать значения объектов при передаче через сеть по протоколу SNMP. Такие таблицы и объекты указаны ниже.

- iptfsInnerStatsTable и iptfsOuterStatsTable. Доступ к статистике внутренних или внешних пакетов IP-TFS может раскрывать сведения, которые IP-TFS желает скрыть, такие как активность потоков, применяющих IP-TFS.

Версии SNMP до SNMPv3 не обеспечивали должной защиты. Даже в защищённой сети (например, использующей IPsec) не контролируется доступ и операции GET (чтение) для объектов этого модуля MIB.

Реализациям **следует** обеспечивать функции защиты, описанные в SNMPv3 [RFC3410], а реализации, заявляющие соответствие стандарту SNMPv3, **должны** включать полную поддержку аутентификации и конфиденциальности с использованием модели защиты по пользователям (User-based Security Model или USM) [RFC3414] с алгоритмом шифрования AES [RFC3826].Реализации **могут** также поддерживать модель транспортной защиты (Transport Security Model или TSM) [RFC5591] в сочетании с защищённым транспортом, таким как SSH [RFC5592] или TLS/DTLS [RFC6353].

Кроме того, развёртывание версий SNMP до SNMPv3 **не рекомендуется**. Взамен **рекомендуется** разворачивать SNMPv3 и включать криптографическую защиту. В дальнейшем клиент (оператор) отвечает за корректную настройку объекта SNMP в части предоставления доступа к экземпляру модуля MIB лишь уполномоченным участникам (пользователям) для выполнения пердусмотренных операций GET или SET (создание, изменение, удаление).

7. Литература

7.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, 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>.

[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>.

[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>.

[RFC9347] Hopps, C., "Aggregation and Fragmentation Mode for Encapsulating Security Payload (ESP) and Its Use for IP Traffic Flow Security (IP-TFS)", RFC 9347, DOI 10.17487/RFC9347, January 2023, <https://www.rfc-editor.org/info/rfc9347>.

7.2. Дополнительная литература

[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>.

[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>.

[RFC9348] Fedyk, D. and C. Hopps, "A YANG Data Model for IP Traffic Flow Security", RFC 9348, DOI 10.17487/RFC9348, January 2023, <https://www.rfc-editor.org/info/rfc9348>.

Благодарности

Авторы благодарны Chris Hopps, Lou Berger, Tero Kivinen за помощь и отклики на модель MIB.

Адреса авторов

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

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

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru