Internet Engineering Task Force (IETF)
Request for Comments: 9348
Category: Standards Track
ISSN: 2070-1721

D. Fedyk
C. Hopps
LabN Consulting, L.L.C.

January 2023

A YANG Data Model for IP Traffic Flow Security

Модель данных YANG для IP Traffic Flow Security

Аннотация

Этот документ описывает модуль YANG для управления дополнениями IP Traffic Flow Security (IP-TFS) для протокола обмена ключами версии 2 (Internet Key Exchange Protocol version 2 или IKEv2) и IPsec.

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/rfc9348.

Авторские права

Copyright (c) 2023. Авторские права принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (http://trustee.ietf.org/license-info), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

Оглавление

1. Введение

Этот документ определяет модуль YANG [RFC7950] для управления расширениями IP Traffic Flow Security (IP-TFS), заданными в [RFC9347]. IP-TFS совершенствует защищённые связи (Security Association или SA) через туннели IPsec для усиления конфиденциальности трафика. Конфиденциальность трафика сокращает возможности его анализа для отождествления и сопоставления наблюдаемых картин трафика. IP-TFS обеспечивает эффективность путём агрегирования трафика в туннельные пакеты IPsec с фиксированным размером.

Модель YANG в этом документе соответствует архитектуре хранилищ данных сетевого управления (Network Management Datastore Architecture или NMDA), заданной в [RFC8342].

Опубликованные модули YANG для IPsec заданы в [RFC9061]. Данный документ использует эти модели в качестве базы для IPsec, которая дополняется для IP-TFS. Модель [RFC9061] поддерживает работу с IKE и без IKE.

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

2. Обзор

Этот документ определяет конфигурационные и рабочие параметры IP-TFS. Расширение IP-TFS, заданное в [RFC9347], определяет защищённые связи для туннельного режима IPsec с характеристиками, усиливающими конфиденциальность трафика и сокращающими снижение потерь пропускной способности. Документы предполагают знакомство читателя с концепциями IPsec, описанными в [RFC4301].

IP-TFS использует туннельный режим для усиления конфиденциальности за счёт сокрытия идентифицируемой информации, размера и времени пакетов. IP-TFS предоставляет базовую возможность агрегирования нескольких пакетов в туннельные пакеты IPsec одинакового размера. Размер внешних пакетов поддерживается за счёт сочетания агрегирования, заполнения и фрагментации внутренних пакетов с целью заполнения внешнего пакета IPsec. Заполнение применяется при отсутствии данных для передачи.

Этот документ задаёт расширяемую модель конфигурации для IP-TFS. Эта версия использует возможности IP-TFS для настройки фиксированного размера пакетов IP-TFS, передаваемых с постоянной скоростью. Модель структурирована для поддержки разных типов операций с помощью будущих дополнений.

Модуль YANG IP-TFS дополняет модуль YANG IPsec из [RFC9061]. IP-TFS использует туннельный режим IPsec и добавляет несколько элементов настройки туннелей IPsec. Как указано в [RFC9347], любая ассоциация SA, настроенная на использование IP-TFS, поддерживает только пакеты IP-TFS (не работает в смешанных режимах IPsec).

Поведение IP-TFS контролируется источником пакетов. Самоописывающий формат пакетов IP-TFS позволяет передающей стороне настраивать размер и время передачи пакетов независимо от получателей. Оба направления трафика независимы, т. е. IP-TFS можно использовать даже в одном направлении. Это означает, что счётчики, заданные здесь для обоих направлений, могут иметь значение 0 или не обновляться, если SA использует IP-TFS лишь в одном направлении.

Ниже указаны случаи, где статистика IP-TFS активна в одном направлении:

- односторонняя SA при включённом IP-TFS;
- двухсторонняя SA с IP-TFS лишь для одного направления.

Статистика IP-TFS доступна для обоих направлений при двухсторонней SA и IP-TFS для обоих направлений.

Модель IP-TFS поддерживает конфигурационные и операционные данные IP-TFS.

Этот модуль YANG поддерживает конфигурацию с фиксированным размером и скоростью пакетов, а также элементы, которые могут быть добавлены для поддержки будущих конфигураций. Спецификация протокола [RFC9347] выходит за рамки этого простого, фиксированного режима работы, задавая базовый формат для любого типа схемы. В этом документе внешние пакеты IPsec могут передаваться с фиксированным или переменным размером (без заполнения). Конфигурация позволяет определять фиксированный размер пакетов на основании MTU для пути. Фиксированный размер пакетов можно также задать в конфигурации, если нужно значение меньше MTU для пути.

Другие элементы конфигурации указаны ниже.

Контроль перегрузки
: Настройки контроля перегрузки, позволяющие IP-TFS снижать скорость пакетов при возникновении перегрузки.

Настройка фиксированной скорости
: Скорость туннеля IP-TFS может настраиваться с учётом издержек уровня L2 или L3. Издержками L3 является скорость данных IP, а издержками L2 является битовая скорость в канале. Сочетание размера пакетов и скорости определяет номинальную максимальную пропускную способность и интервал передачи при использовании пакетов фиксированного размера.

Пользовательский контроль фрагментации пакетов
: Хотя фрагментация рекомендуется для повышения эффективности, возможна её настройка, если пользователи хотят видеть влияние отказа от фрагментации на свои потоки данных.

Рабочие данные YANG позволяют считывать параметры конфигурации, а также статистику на уровне SA и счётчики ошибок для IP-TFS. Статистика пакетов IPsec на уровне SA обеспечивается как свойство, а статистика IP-TFS на уровне SA - как другое свойство. Оба набора статистики дополняют модули YANG IPsec счётчиками, которые позволяют наблюдать эффективность пакетов IP-TFS.

Объекты управления YANG IPsec заданы в [RFC9061]. YANG IP-TFS дополняет модели IKE и без IKE. В этих моделях запись базы данных правил безопасности (Security Policy) и запись SA для туннеля IPsec могут дополняться IP-TFS. Кроме того, эта модель YANG использует типы, определённые в [RFC6991].

3. Управление YANG

3.1. Дерево YANG

Ниже представлено дерево YANG [RFC8340] для расширений IP-TFS.

```
module: ietf-ipsec-iptfs
  augment /nsfike:ipsec-ike/nsfike:conn-entry/nsfike:spd
            /nsfike:spd-entry/nsfike:ipsec-policy-config
            /nsfike:processing-info/nsfike:ipsec-sa-cfg:
    +--rw traffic-flow-security
       +--rw congestion-control?           boolean
       +--rw packet-size
       |  +--rw use-path-mtu-discovery?   boolean
       |  +--rw outer-packet-size?        uint16
       +--rw (tunnel-rate)?
       |  +--:(l2-fixed-rate)
       |  |  +--rw l2-fixed-rate?          yang:gauge64
       |  +--:(l3-fixed-rate)
       |     +--rw l3-fixed-rate?          yang:gauge64
```

```
        +--rw dont-fragment?                boolean
        +--rw max-aggregation-time?         decimal64
        +--rw window-size?                  uint16
        +--rw send-immediately?             boolean
        +--rw lost-packet-timer-interval?   decimal64
    augment /nsfike:ipsec-ike/nsfike:conn-entry/nsfike:child-sa-info:
      +--ro traffic-flow-security
        +--ro congestion-control?           boolean
        +--ro packet-size
        |  +--ro use-path-mtu-discovery?   boolean
        |  +--ro outer-packet-size?        uint16
        +--ro (tunnel-rate)?
        |  +--:(l2-fixed-rate)
        |  |  +--ro l2-fixed-rate?          yang:gauge64
        |  +--:(l3-fixed-rate)
        |     +--ro l3-fixed-rate?          yang:gauge64
        +--ro dont-fragment?                boolean
        +--ro max-aggregation-time?         decimal64
        +--ro window-size?                  uint16
        +--ro send-immediately?             boolean
        +--ro lost-packet-timer-interval?   decimal64
    augment /nsfikels:ipsec-ikeless/nsfikels:spd/nsfikels:spd-entry
              /nsfikels:ipsec-policy-config/nsfikels:processing-info
              /nsfikels:ipsec-sa-cfg:
      +--rw traffic-flow-security
        +--rw congestion-control?           boolean
        +--rw packet-size
        |  +--rw use-path-mtu-discovery?   boolean
        |  +--rw outer-packet-size?        uint16
        +--rw (tunnel-rate)?
        |  +--:(l2-fixed-rate)
        |  |  +--rw l2-fixed-rate?          yang:gauge64
        |  +--:(l3-fixed-rate)
        |     +--rw l3-fixed-rate?          yang:gauge64
        +--rw dont-fragment?                boolean
        +--rw max-aggregation-time?         decimal64
        +--rw window-size?                  uint16
        +--rw send-immediately?             boolean
        +--rw lost-packet-timer-interval?   decimal64
    augment /nsfikels:ipsec-ikeless/nsfikels:sad/nsfikels:sad-entry:
      +--ro traffic-flow-security
        +--ro congestion-control?           boolean
        +--ro packet-size
        |  +--ro use-path-mtu-discovery?   boolean
        |  +--ro outer-packet-size?        uint16
        +--ro (tunnel-rate)?
        |  +--:(l2-fixed-rate)
        |  |  +--ro l2-fixed-rate?          yang:gauge64
        |  +--:(l3-fixed-rate)
        |     +--ro l3-fixed-rate?          yang:gauge64
        +--ro dont-fragment?                boolean
        +--ro max-aggregation-time?         decimal64
        +--ro window-size?                  uint16
        +--ro send-immediately?             boolean
        +--ro lost-packet-timer-interval?   decimal64
    augment /nsfike:ipsec-ike/nsfike:conn-entry/nsfike:child-sa-info:
      +--ro ipsec-stats {ipsec-stats}?
      |  +--ro tx-pkts?         yang:counter64
      |  +--ro tx-octets?       yang:counter64
      |  +--ro tx-drop-pkts?    yang:counter64
      |  +--ro rx-pkts?         yang:counter64
      |  +--ro rx-octets?       yang:counter64
      |  +--ro rx-drop-pkts?    yang:counter64
      +--ro iptfs-inner-pkt-stats {iptfs-stats}?
      |  +--ro tx-pkts?              yang:counter64
      |  +--ro tx-octets?            yang:counter64
      |  +--ro rx-pkts?              yang:counter64
      |  +--ro rx-octets?            yang:counter64
      |  +--ro rx-incomplete-pkts?   yang:counter64
      +--ro iptfs-outer-pkt-stats {iptfs-stats}?
        +--ro tx-all-pad-pkts?       yang:counter64
        +--ro tx-all-pad-octets?     yang:counter64
        +--ro tx-extra-pad-pkts?     yang:counter64
        +--ro tx-extra-pad-octets?   yang:counter64
        +--ro rx-all-pad-pkts?       yang:counter64
        +--ro rx-all-pad-octets?     yang:counter64
        +--ro rx-extra-pad-pkts?     yang:counter64
        +--ro rx-extra-pad-octets?   yang:counter64
        +--ro rx-errored-pkts?       yang:counter64
        +--ro rx-missed-pkts?        yang:counter64
    augment /nsfikels:ipsec-ikeless/nsfikels:sad/nsfikels:sad-entry:
      +--ro ipsec-stats {ipsec-stats}?
      |  +--ro tx-pkts?         yang:counter64
      |  +--ro tx-octets?       yang:counter64
      |  +--ro tx-drop-pkts?    yang:counter64
      |  +--ro rx-pkts?         yang:counter64
```

```
      |  +--ro rx-octets?      yang:counter64
      |  +--ro rx-drop-pkts?   yang:counter64
      +--ro iptfs-inner-pkt-stats {iptfs-stats}?
      |  +--ro tx-pkts?              yang:counter64
      |  +--ro tx-octets?            yang:counter64
      |  +--ro rx-pkts?              yang:counter64
      |  +--ro rx-octets?            yang:counter64
      |  +--ro rx-incomplete-pkts?   yang:counter64
      +--ro iptfs-outer-pkt-stats {iptfs-stats}?
         +--ro tx-all-pad-pkts?       yang:counter64
         +--ro tx-all-pad-octets?     yang:counter64
         +--ro tx-extra-pad-pkts?     yang:counter64
         +--ro tx-extra-pad-octets?   yang:counter64
         +--ro rx-all-pad-pkts?       yang:counter64
         +--ro rx-all-pad-octets?     yang:counter64
         +--ro rx-extra-pad-pkts?     yang:counter64
         +--ro rx-extra-pad-octets?   yang:counter64
         +--ro rx-errored-pkts?       yang:counter64
         +--ro rx-missed-pkts?        yang:counter64
```

3.2. Модуль YANG

Ниже представлен модуль YANG для управления расширениями IP-TFS. Эта модель ссылается на [RFC9347] и [RFC5348].

```
<CODE BEGINS> file "ietf-ipsec-iptfs@2023-01-31.yang"
module ietf-ipsec-iptfs {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-ipsec-iptfs";
  prefix iptfs;

  import ietf-i2nsf-ike {
    prefix nsfike;
    reference
      "RFC 9061: A YANG Data Model for IPsec Flow Protection Based on
       Software-Defined Networking (SDN), параграф 5.2";
  }
  import ietf-i2nsf-ikeless {
    prefix nsfikels;
    reference
      "RFC 9061: A YANG Data Model for IPsec Flow Protection Based on
       Software-Defined Networking (SDN), параграф 5.3";
  }
  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991: Common YANG Data Types";
  }

  organization
    "IETF IPSECME Working Group (IPSECME)";
  contact
    "WG Web:  <https://datatracker.ietf.org/wg/ipsecme/>
     WG List: <mailto:ipsecme@ietf.org>

     Author: Don Fedyk
             <mailto:dfedyk@labn.net>

     Author: Christian Hopps
             <mailto:chopps@chopps.org>";

  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 YANG является частью RFC 9348, где правовые
     аспекты приведены более полно.";

  revision 2023-01-31 {
    description
      "Исходный выпуск";
    reference
      "RFC 9348: A YANG Data Model for IP Traffic Flow Security";
  }

  feature ipsec-stats {
    description
      "Указывает поддержку устройством статистики для IPsec SA.";
```

```
  }

  feature iptfs-stats {
    description
      "Указывает поддержку устройством статистики IP TFS для SA.";
  }

  /*--------------------*/
  /*   Группировки      */
  /*--------------------*/

  grouping ipsec-tx-stat-grouping {
    description
      "Выходная статистика IPsec";
    leaf tx-pkts {
      type yang:counter64;
      config false;
      description
        "Счётчик выходных пакетов";
    }
    leaf tx-octets {
      type yang:counter64;
      config false;
      description
        "Число байтов в выходных пакетах";
    }
    leaf tx-drop-pkts {
      type yang:counter64;
      config false;
      description
        "Число отброшенных выходных пакетов";
    }
  }

  grouping ipsec-rx-stat-grouping {
    description
      "Входная статистика IPsec";
    leaf rx-pkts {
      type yang:counter64;
      config false;
      description
        "Счётчик входных пакетов";
    }
    leaf rx-octets {
      type yang:counter64;
      config false;
      description
        "Число байтов в входных пакетах";
    }
    leaf rx-drop-pkts {
      type yang:counter64;
      config false;
      description
        "Число отброшенных входных пакетов";
    }
  }

  grouping iptfs-inner-tx-stat-grouping {
    description
      "Статистика вложенных выходных пакетов IP-TFS";
    leaf tx-pkts {
      type yang:counter64;
      config false;
      description
        "Общее число переданных вложенных пакетов IP-TFS. Учитываются
         только целые пакеты, все фрагменты пакета считаются за 1.";
      reference
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS)";
    }
    leaf tx-octets {
      type yang:counter64;
      config false;
      description
        "Общее число переданных вложенных октетов IP-TFS. Заполнение
         не учитывается.";
      reference
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS)";
    }
  }

  grouping iptfs-outer-tx-stat-grouping {
    description
```

```
        "Статистика выходных вложенных пакетов IP-TFS.";
      leaf tx-all-pad-pkts {
        type yang:counter64;
        config false;
        description
          "Общее число переданных пакетов IP-TFS, содержавших только
           заполнение (без данных).";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 2.2.3";
      }
      leaf tx-all-pad-octets {
        type yang:counter64;
        config false;
        description
          "Общее число переданных октетов заполнения в пакетах IP-TFS
           без вложенных данных.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 2.2.3";
      }
      leaf tx-extra-pad-pkts {
        type yang:counter64;
        config false;
        description
          "Общее число переданных внешних пакетов IP-TFS, содержащих
           заполнение.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 2.2.3.1";
      }
      leaf tx-extra-pad-octets {
        type yang:counter64;
        config false;
        description
          "Общее число переданных октетов заполнения, добавленных во
           внешние пакеты IP-TFS с данными.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 2.2.3.1";
      }
    }

    grouping iptfs-inner-rx-stat-grouping {
      description
        "Входная статистика вложенных пакетов IP-TFS";
      leaf rx-pkts {
        type yang:counter64;
        config false;
        description
          "Общее число полученных вложенных пакетов IP-TFS.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 2.2";
      }
      leaf rx-octets {
        type yang:counter64;
        config false;
        description
          "Общее число принятых вложенных октетов IP-TFS без учёта
           заполнения и издержек.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 2.2";
      }
      leaf rx-incomplete-pkts {
        type yang:counter64;
        config false;
        description
          "Общее число неполных вложенных пакетов IP-TFS. Обычно это
           возникает в результате пропуска фрагментов и может быть
           следствием нарушения порядка или ошибок в полученных внешних
           пакетах.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS)";
      }
    }
```

```
  grouping iptfs-outer-rx-stat-grouping {
    description
      "Входная статистика внешних пакетов IP-TFS";
    leaf rx-all-pad-pkts {
      type yang:counter64;
      config false;
      description
        "Общее число полученных пакетов IP-TFS, содержащих лишь
         заполнение (без данных).";
      reference
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS), Section 2.2.3";
    }
    leaf rx-all-pad-octets {
      type yang:counter64;
      config false;
      description
        "Общее число полученных октетов заполнения, добавленных
         в пакеты IP-TFS без вложенных данных.";
      reference
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS), Section 2.2.3";
    }
    leaf rx-extra-pad-pkts {
      type yang:counter64;
      config false;
      description
        "Общее число принятых внешних пакетов IP-TFS с заполнением.";
      reference
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS), Section 2.2.3.1";
    }
    leaf rx-extra-pad-octets {
      type yang:counter64;
      config false;
      description
        "Общее число полученных октетов заполнения, добавленных во
         внешние пакеты IP-TFS с данными.";
      reference
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS), Section 2.2.3.1";
    }
    leaf rx-errored-pkts {
      type yang:counter64;
      config false;
      description
        "Общее число внешних пакетов IP-TFS, отброшенных из-за
         ошибок.";
      reference
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS)";
    }
    leaf rx-missed-pkts {
      type yang:counter64;
      config false;
      description
        "Общее число отсутствующих внешних пакетов IP-TFS, указанное
         отсутствующим порядковым номером.";
      reference
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS)";
    }
  }

  grouping iptfs-config {
    description
      "Группировка для конфигурации IP-TFS.";
    container traffic-flow-security {
      description
        "Настраивает IPsec TFS в базе SAD.";
      leaf congestion-control {
        type boolean;
        default "true";
        description
          "Принятое по умолчанию значение true включает обмен данными
           о перегрузке в линии, которые нужны алгоритмам контроля
           перегрузок, как указано в RFC 5348. При установке false
           IP-TFS передаёт пакеты фиксированного размера через
           туннель IP-TFS с постоянной скоростью.";
        reference
```

```
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS), Section 2.4.2;
         RFC 5348: TCP Friendly Rate Control (TFRC): Protocol
         Specification";
    }
    container packet-size {
      description
        "Размер пакетов задаётся вручную или определяется
         автоматически.";
      leaf use-path-mtu-discovery {
        type boolean;
        default "true";
        description
          "Применяется определение MTU на пути для задания
           максимального размера пакетов IP-TFS. Если размер задан
           явно, при установке use-path-mtu-discovery он может лишь
           сокращаться.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 4.2";
      }
      leaf outer-packet-size {
        type uint16;
        units "bytes";
        description
          "Размер внешнего инкапсулирующего пакета при передаче
           (т. е. пакета IP с содержимым ESP).";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 4.2";
      }
    }
    choice tunnel-rate {
      description
        "Битовая скорость TFS может быть задана скоростью линии L2
         или скоростью пакетов L3.";
      leaf l2-fixed-rate {
        type yang:gauge64;
        units "bits/second";
        description
          "Целевая пропускная способность/битовая скорость туннеля
           IP-TFS при передаче в бит/сек. Эта фиксированная скорость
           задаёт номинальное время передачи пакетов фиксированного
           размера. Если включён контроль перегрузок, скорость может
           снижаться (или увеличиваться, если не была задана).";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 4.1";
      }
      leaf l3-fixed-rate {
        type yang:gauge64;
        units "bits/second";
        description
          "Целевая пропускная способность/битовая скорость туннеля
           IP-TFS при передаче в бит/сек. Эта фиксированная скорость
           задаёт номинальное время передачи пакетов фиксированного
           размера. Если включён контроль перегрузок, скорость может
           снижаться (или увеличиваться, если не была задана).";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 4.1";
      }
    }
    leaf dont-fragment {
      type boolean;
      default "false";
      description
        "При передаче отключает фрагментацию между
         последовательными пакетами туннеля IP-TFS. Внутренние
         пакеты, не помещающиеся во внешний пакет, отбрасываются.";
      reference
        "RFC 9347: Aggregation and Fragmentation Mode for
         Encapsulating Security Payload (ESP) and Its Use for
         IP Traffic Flow Security (IP-TFS), Section 2.2.4 and
         6.1.4";
    }
    leaf max-aggregation-time {
      type decimal64 {
        fraction-digits 6;
      }
      units "milliseconds";
```

```
        description
          "При передаче максимальным временем агрегирования является
           максимальное время удержания полученного внутреннего
           пакета до передачи в туннеле IP-TFS. Внутренние пакеты,
           которые удерживаются дольше этого времени, исходя из
           текущей конфигурации, будут отбрасываться вместо включения
           в очередь передачи. Максимальное время агрегирования
           задаётся в миллисекундах или долях миллисекунды вплоть
           до 1 наносекунды.";
      }
      leaf window-size {
        type uint16 {
          range "0..65535";
        }
        description
          "Максимальное число полученных с нарушением порядка пакетов,
           для которых получатель IP-TFS будет восстанавливать порядок.
           Значение 0 отключает восстановление порядка.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 2.2.3";
      }
      leaf send-immediately {
        type boolean;
        default "false";
        description
          "Задаёт максимально быструю отправку пакетов при получении
           без ожидания потерянных и разупорядоченных внешних пакетов.
           Выбор этой опции сокращает задержку вложенных
           (пользовательских) пакетов, но усиливает нарушение порядка
           доставки потока вложенных пакетов при наличии
           агрегирования или нарушения порядка.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 2.5";
      }
      leaf lost-packet-timer-interval {
        type decimal64 {
          fraction-digits 6;
        }
        units "milliseconds";
        description
          "При получении задаёт время ожидания получателем IP-TFS
           пропущенного пакета, прежде чем счесть его потерянным.
           Если не задан лист send-immediately, каждый потерянный
           пакет будет задерживать внутренние (пользовательские)
           пакеты, пока не наступит этот тайм-аут. Установка слишком
           малого значения может влиять на восстановление порядка и
           сборку. Значение задаётся в миллисекундах или долях
           миллисекунды вплоть до 1 наносекунды.";
        reference
          "RFC 9347: Aggregation and Fragmentation Mode for
           Encapsulating Security Payload (ESP) and Its Use for
           IP Traffic Flow Security (IP-TFS), Section 2.2.3";
      }
    }
  }

  /*
   * Крнфигурация IP-TFS IKE
   */

  augment "/nsfike:ipsec-ike/nsfike:conn-entry/nsfike:spd/"
        + "nsfike:spd-entry/"
        + "nsfike:ipsec-policy-config/"
        + "nsfike:processing-info/"
        + "nsfike:ipsec-sa-cfg" {
    description
      "Конфигурация IP-TFS для этого правила.";
    uses iptfs-config;
  }

  augment "/nsfike:ipsec-ike/nsfike:conn-entry/"
        + "nsfike:child-sa-info" {
    description
      "IP-TFS настроено для этой SA.";
    uses iptfs-config {
      refine "traffic-flow-security" {
        config false;
      }
    }
  }

  /*
```

```
     * Конфигурация IP-TFS без IKE
     */

    augment "/nsfikels:ipsec-ikeless/nsfikels:spd/"
          + "nsfikels:spd-entry/"
          + "nsfikels:ipsec-policy-config/"
          + "nsfikels:processing-info/"
          + "nsfikels:ipsec-sa-cfg" {
      description
        "Конфигурация IP-TFS для этого правила.";
      uses iptfs-config;
    }

    augment "/nsfikels:ipsec-ikeless/nsfikels:sad/"
          + "nsfikels:sad-entry" {
      description
        "IP-TFS настроено для этой SA.";
      uses iptfs-config {
        refine "traffic-flow-security" {
          config false;
        }
      }
    }

    /*
     * Счётчики пакетов
     */

    augment "/nsfike:ipsec-ike/nsfike:conn-entry/"
          + "nsfike:child-sa-info" {
      description
        "Счётчики на уровне SA";
      container ipsec-stats {
        if-feature "ipsec-stats";
        config false;
        description
          "Счётчики пакетов IPsec на уровне SA.
           tx = выходные, rx = входные";
        uses ipsec-tx-stat-grouping;
        uses ipsec-rx-stat-grouping;
      }
      container iptfs-inner-pkt-stats {
        if-feature "iptfs-stats";
        config false;
        description
          "Счётчики внутренних пакетов IP-TFS на уровне SA.
           tx = выходные, rx = входные";
        uses iptfs-inner-tx-stat-grouping;
        uses iptfs-inner-rx-stat-grouping;
      }
      container iptfs-outer-pkt-stats {
        if-feature "iptfs-stats";
        config false;
        description
          "Счётчики внешних пакетов IP-TFS на уровне SA.
           tx = выходные, rx = входные";
        uses iptfs-outer-tx-stat-grouping;
        uses iptfs-outer-rx-stat-grouping;
      }
    }

    /*
     * Счётчики пакетов
     */

    augment "/nsfikels:ipsec-ikeless/nsfikels:sad/"
          + "nsfikels:sad-entry" {
      description
        "Счётчики на уровне SA";
      container ipsec-stats {
        if-feature "ipsec-stats";
        config false;
        description
          "Счётчики пакетов IPsec на уровне SA.
           tx = выходные, rx = входные";
        uses ipsec-tx-stat-grouping;
        uses ipsec-rx-stat-grouping;
      }
      container iptfs-inner-pkt-stats {
        if-feature "iptfs-stats";
        config false;
        description
          "Счётчики внутренних пакетов IP-TFS на уровне SA.
           tx = выходные, rx = входные";
        uses iptfs-inner-tx-stat-grouping;
        uses iptfs-inner-rx-stat-grouping;
```

```
      }
      container iptfs-outer-pkt-stats {
        if-feature "iptfs-stats";
        config false;
        description
          "Счётчики внешних пакетов IP-TFS на уровне SA.
           tx = выходные, rx = входные";
        uses iptfs-outer-tx-stat-grouping;
        uses iptfs-outer-rx-stat-grouping;
      }
    }
  }
  <CODE ENDS>
```

4. Взаимодействие с IANA

4.1. Обновление реестра IETF XML

В соответствии с этим документом агентство IANA зарегистрировало URI в реестре IETF XML Registry [RFC3688]

```
URI:  urn:ietf:params:xml:ns:yang:ietf-ipsec-iptfs
Registrant Contact:  The IESG.
XML:  N/A; запрошенный URI является пространством имён XML.
```

4.2. Обновление реестра YANG Module Names

В соответствии с этим документом агентство IANA зарегистрировало модуль YANG в реестре YANG Module Names [RFC6020]

```
Name:  ietf-ipsec-iptfs
Namespace:  urn:ietf:params:xml:ns:yang:ietf-ipsec-iptfs
Prefix:  iptfs
Reference:  RFC 9348
```

5. Вопросы безопасности

Заданный этим документом модуль YANG определяет схему для данных, предназначенную для доступа через сеть с использованием протоколов управления, таких как NETCONF [RFC6241] или RESTCONF [RFC8040]. Нижним уровнем NETCONF служит защищённый транспорт с обязательной поддержкой SSH (Secure Shell) [RFC6242]. Нижним уровнем RESTCONF служит протокол HTTPS с обязательной поддержкой защиты на транспортном уровне (TLS) [RFC8446].

Модель доступа к конфигурации сети (NACM – Network Configuration Access Control Model) [RFC8341] обеспечивает возможность разрешить доступ лишь определённых пользователей NETCONF или RESTCONF к заранее заданному подмножеству операций NETCONF или RESTCONF и содержимого.

В этом модуле данных YANG определено множество узлов данных, которые разрешают запись, создание и удаление (т. е. config true, как принято по умолчанию). Эти узлы могут быть конфиденциальными или уязвимыми в некоторых сетевых средах. Запись в такие узлы (например, edit-config) без должной защиты может негативно влиять на работу сети. Ниже перечислены ветви и узлы, которые могут быть конфиденциальны или уязвимы.

../traffic-flow-security

Включение IP-TFS контролируется установкой записей в ветви traffic-flow-security моделей с IKE или без IKE. Параметры в этом дереве устанавливаются для IP-TFS чувствительность к перегрузкам или фиксированную скорость.

Некоторые из доступных для чтения узлов в этом модуле YANG могут быть конфиденциальны или уязвимы в той или иной сетевой среде. Важно контролировать доступ к таким объектам (например, get, get-config, notification). Ниже перечислены ветви и узлы, которые могут быть конфиденциальны или уязвимы.

../iptfs-inner-pkt-stats и ../iptfs-outer-pkt-stats

Доступ к статистике IP-TFS даёт сведения о событиях IP-TFS, таких как корректная работа потоков IP-TFS.

6. Литература

6.1. Нормативные документы

[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>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <https://www.rfc-editor.org/info/rfc8342>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9061] Marin-Lopez, R., Lopez-Millan, G., and F. Pereniguez-Garcia, "A YANG Data Model for IPsec Flow Protection Based on Software-Defined Networking (SDN)", RFC 9061, DOI 10.17487/RFC9061, July 2021, <https://www.rfc-editor.org/info/rfc9061>.

[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>.

6.2. Дополнительная литература

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[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>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

Приложение A. Примеры

Ниже приведены примеры данных конфигурации и рабочего состояния для вариантов использования с IKE и без IKE в формате XML и JSON. Показана также операционная статистика для варианта без IKE.

A.1. Конфигурация XML

Этот пример показывает конфигурацию IP-TFS для варианта без IKE. Отметим, что это дополняет схему для IPsec без IKE, поэтому задана лишь минимальная конфигурация для схемы без IKE.

```
<i:ipsec-ikeless
  xmlns:i="urn:ietf:params:xml:ns:yang:ietf-i2nsf-ikeless"
  xmlns:tfs="urn:ietf:params:xml:ns:yang:ietf-ipsec-iptfs">
  <i:spd>
    <i:spd-entry>
      <i:name>protect-policy-1</i:name>
      <i:direction>outbound</i:direction>
      <i:ipsec-policy-config>
        <i:traffic-selector>
          <i:local-prefix>192.0.2.0/16</i:local-prefix>
          <i:remote-prefix>198.51.100.0/16</i:remote-prefix>
        </i:traffic-selector>
        <i:processing-info>
          <i:action>protect</i:action>
          <i:ipsec-sa-cfg>
            <tfs:traffic-flow-security>
             <tfs:congestion-control>true</tfs:congestion-control>
              <tfs:packet-size>
                <tfs:use-path-mtu-discovery
                   >true</tfs:use-path-mtu-discovery>
              </tfs:packet-size>
              <tfs:l2-fixed-rate>1000000000</tfs:l2-fixed-rate>
              <tfs:max-aggregation-time
                 >0.1</tfs:max-aggregation-time>
              <tfs:window-size>5</tfs:window-size>
              <tfs:send-immediately>false</tfs:send-immediately>
              <tfs:lost-packet-timer-interval
                 >0.2</tfs:lost-packet-timer-interval>
            </tfs:traffic-flow-security>
          </i:ipsec-sa-cfg>
        </i:processing-info>
      </i:ipsec-policy-config>
    </i:spd-entry>
  </i:spd>
</i:ipsec-ikeless>
```

Рисунок 1. Пример конфигурации IP-TFS XML.

A.2. Рабочие данные XML

Этот пример показывает рабочие данные для варианта IP-TFS без IKE. Отметим, что это дополняет схему для IPsec без IKE, поэтому задана лишь минимальная конфигурация для схемы без IKE.

```
<i:ipsec-ikeless
  xmlns:i="urn:ietf:params:xml:ns:yang:ietf-i2nsf-ikeless"
  xmlns:tfs="urn:ietf:params:xml:ns:yang:ietf-ipsec-iptfs">
  <i:sad>
    <i:sad-entry>
      <i:name>sad-1</i:name>
      <i:ipsec-sa-config>
        <i:spi>1</i:spi>
```

```
          <i:traffic-selector>
            <i:local-prefix>2001:db8:1::/48</i:local-prefix>
            <i:remote-prefix>2001:db8:2::/48</i:remote-prefix>
          </i:traffic-selector>
        </i:ipsec-sa-config>
        <tfs:traffic-flow-security>
          <tfs:congestion-control>true</tfs:congestion-control>
          <tfs:packet-size>
            <tfs:use-path-mtu-discovery
              >true</tfs:use-path-mtu-discovery>
          </tfs:packet-size>
          <tfs:l2-fixed-rate>1000000000</tfs:l2-fixed-rate>
          <tfs:max-aggregation-time>0.100</tfs:max-aggregation-time>
          <tfs:window-size>0</tfs:window-size>
          <tfs:send-immediately>true</tfs:send-immediately>
          <tfs:lost-packet-timer-interval
            >0.200</tfs:lost-packet-timer-interval>
        </tfs:traffic-flow-security>
      </i:sad-entry>
    </i:sad>
  </i:ipsec-ikeless>
```

Рисунок 2. Пример рабочих данных IP-TFS XML.

A.3. Конфигурация JSON

Этот пример показывает данные конфигурации для IP-TFS с IKE. Отметим, что это дополняет схему IPsec IKE, , поэтому задана лишь минимальная конфигурация для схемы с IKE.

```
{
  "ietf-i2nsf-ike:ipsec-ike": {
    "ietf-i2nsf-ike:conn-entry": [
      {
        "name": "my-peer-connection",
        "ike-sa-encr-alg": [
          {
            "id": 1,
            "algorithm-type": 12,
            "key-length": 128
          }
          ],
          "local": {
            "local-pad-entry-name": "local-1"
          },
          "remote": {
            "remote-pad-entry-name": "remote-1"
          },
          "ietf-i2nsf-ike:spd": {
          "spd-entry": [
            {
              "name": "protect-policy-1",
              "ipsec-policy-config": {
                "traffic-selector": {
                  "local-prefix": "192.0.2.0/16",
                  "remote-prefix": "198.51.100.0/16"
                },
                "processing-info": {
                  "action": "protect",
                  "ipsec-sa-cfg": {
                    "ietf-ipsec-iptfs:traffic-flow-security": {
                      "congestion-control": true,
                      "l2-fixed-rate": "1000000000",
                      "packet-size": {
                        "use-path-mtu-discovery": true
                      },
                      "max-aggregation-time": "0.1",
                      "window-size": 1,
                      "send-immediately": false,
                      "lost-packet-timer-interval": "0.2"
                    }
                  }
                }
              }
            }
          ]
        }
      }
    ]
  }
}
```

Рисунок 3. Пример конфигурации IP-TFS JSON.

A.4. Рабочие данные JSON

Этот пример показывает рабочие данные для варианта IP-TFS с IKE. Отметим, что это дополняет схему IPsec IKE, , поэтому задана лишь минимальная конфигурация для схемы с IKE.

```
{
  "ietf-i2nsf-ike:ipsec-ike": {
    "ietf-i2nsf-ike:conn-entry": [
      {
        "name": "my-peer-connection",
        "ike-sa-encr-alg": [
        {
          "id": 1,
          "algorithm-type": 12,
          "key-length": 128
        }
        ],
        "local": {
          "local-pad-entry-name": "local-1"
        },
        "remote": {
          "remote-pad-entry-name": "remote-1"
        },
        "ietf-i2nsf-ike:child-sa-info": {
          "ietf-ipsec-iptfs:traffic-flow-security": {
            "congestion-control": true,
            "l2-fixed-rate": "1000000000",
            "packet-size": {
              "use-path-mtu-discovery": true
            },
            "max-aggregation-time": "0.1",
            "window-size": 5,
            "send-immediately": false,
            "lost-packet-timer-interval": "0.2"
          }
        }
      }
    ]
  }
}
```

Рисунок 4. Пример операционных данных IP-TFS JSON.

A.5. Операционная статистика JSON

Этот пример показывает статистику IP-TFS в формате JSON. Отметим, что показана передающая сторона двухстороннего IP-TFS в произвольными номерами при передаче.

```
{
  "ietf-i2nsf-ikeless:ipsec-ikeless": {
    "sad": {
      "sad-entry": [
        {
          "name": "sad-1",
          "ipsec-sa-config": {
            "spi": 1,
            "traffic-selector": {
              "local-prefix": "192.0.2.1/16",
              "remote-prefix": "198.51.100.0/16"
            }
          },
          "ietf-ipsec-iptfs:traffic-flow-security": {
            "window-size": 5,
            "send-immediately": false,
            "lost-packet-timer-interval": "0.2"
          },
          "ietf-ipsec-iptfs:ipsec-stats": {
            "tx-pkts": "300",
            "tx-octets": "80000",
            "tx-drop-pkts": "2",
            "rx-pkts": "0",
            "rx-octets": "0",
            "rx-drop-pkts": "0"
          },
          "ietf-ipsec-iptfs:iptfs-inner-pkt-stats": {
            "tx-pkts": "250",
            "tx-octets": "75000",
            "rx-pkts": "0",
            "rx-octets": "0",
            "rx-incomplete-pkts": "0"
          },
          "ietf-ipsec-iptfs:iptfs-outer-pkt-stats": {
            "tx-all-pad-pkts": "40",
            "tx-all-pad-octets": "40000",
            "tx-extra-pad-pkts": "200",
            "tx-extra-pad-octets": "30000",
            "rx-all-pad-pkts": "0",
```

```
              "rx-all-pad-octets": "0",
              "rx-extra-pad-pkts": "0",
              "rx-extra-pad-octets": "0",
              "rx-errored-pkts": "0",
              "rx-missed-pkts": "0"
            },
            "ipsec-sa-state": {
              "sa-lifetime-current": {
                "time": 80000,
                "bytes": "400606",
                "packets": 1000,
                "idle": 5
              }
            }
          }
        ]
      }
    }
  }
```

Рисунок 5. Пример статистики IP-TFS JSON.

Благодарности

Авторы благодарны Eric Kinzie, Jürgen Schönwälder, Lou Berger, Tero Kivinen за отклики и рецензии на модуль YANG.

Адреса авторов

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

Christian Hopps
LabN Consulting, L.L.C.
Email: chopps@chopps.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru