Donald Fedyk
Christian Hopps
LabN Consulting, LLC

YANG Model for IP Traffic Flow Security

IETF 109 – “draft-fedyk-ipsecme-yang-iptfs-01”

Changes since IETF108

- Some reminders
  - Draft objective -- YANG support for IP-TFS
    - Expect to also do a derivative SNMP draft
  - Draft approach – Augment existing IPsec YANG model
    - ietf-i2nsf-sdn-ipsec-flow-protection
- Open issue with base YANG model discussed at last meeting resolved
  - Base yang model focused on controller use case
  - Previous version was incompatible with device configuration
  - Based on comments, incompatible usage was made a YANG feature
    - Now usable as foundation for TFS device configuration
  - Draft updated to align with ietf-i2nsf-sdn-ipsec-flow-protection changes
    - https://tools.ietf.org/rfcdiff?difftype=--hwdiff&url2=draft-ietf-i2nsf-sdn-ipsec-flow-protection-10.txt

More details on draft-ietf-i2nsf-sdn-ipsec-flow-protection

- https://tools.ietf.org/html/draft-ietf-i2nsf-sdn-ipsec-flow-protection-12
- I2NSF WG defined SDN model provides for an IKE and IKE-less operation
- IKE module intentionally missing a Security Association Database
  - Reason given: centralized controller (SDN) doesn't care about SAs
  - Has `child-sa-info` to hold connections SA related info
- IKE module missing SA information
  - `child-sa-info` only has pfs-groups and lifetime values
  - no information on selected transforms, etc
- Existing model (IKE/IKE-less) does not have Basic IPsec counters
- IP-TFS YANG augments this model

IP-TFS Configuration

- Congestion Control
  - Boolean
- Packet Size (L3 Packet size)
  - Fixed Size
  - Use Path MTU (set or lowers fixed)
- Bit rate
  - L3 Bit rate or
  - L2 Bit rate
- Allow fragmentation
  - Of Inner packets using data blocks and IP TFS offsets

Packet Transmission Frequency = Bit rate/Packet size

Note these are minimal controls vendors or future work may augment

Operational Statistics

- Outer IPsec Packet – IPsec Counters
  - tx IPsec packets and octets
  - rx IPsec packets and octets
  - rx dropped packet counts
  - rx error counts/type
- Inner IP Packets – IP-TFS Counters
  - tx packets and octets
  - tx extra pad packets and octets
  - tx all pad packets and octets
  - rx packets and octets
  - rx extra pad packets and octets
  - rx all pad packets and octets
  - rx errored packets
  - rx missed packets
  - rx incomplete inner packets

IP-TFS Protocol Overhead = Outer Packet Octets - Inner Packet Octets - Pad Octets

Next Steps

- Authors request WG adoption

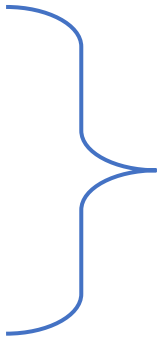
Comments / Questions?

More Details

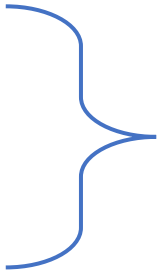
IP-TFS Config augment `nsfike`

```
module: ietf-ipsecme-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?        boolean
       |  +--rw outer-packet-size?   uint16
       +--rw (tunnel-rate)?
       |  +--:(l2-bitrate)
       |  |  +--rw l2-bitrate?     uint64
       |  +--:(l3-bitrate)
       |     +--rw l3-bitrate?     uint64
       +--rw dont-fragment?        boolean

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?        boolean
       |  +--ro outer-packet-size?   uint16
       +--ro (tunnel-rate)?
       |  +--:(l2-bitrate)
       |  |  +--ro l2-bitrate?     uint64
       |  +--:(l3-bitrate)
       |     +--ro l3-bitrate?     uint64
       +--ro dont-fragment?        boolean
```



User Provided Config



Operational (Actual) Config

IP-TFS Config augment `nfs-ikels`

```
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?        boolean
       |  +--rw outer-packet-size?   uint16
       +--rw (tunnel-rate)?
       |  +--:(l2-bitrate)
       |  |  +--rw l2-bitrate?     uint64
       |  +--:(l3-bitrate)
       |     +--rw l3-bitrate?     uint64
       +--rw dont-fragment?        boolean

 augment /nsfikels:ipsec-ikeless
         /nsfikels:sad/nsfikels:sad-entry:
    +--ro traffic-flow-security
       +--ro congestion-control?   boolean
       +--ro packet-size
       |  +--ro use-path-mtu?        boolean
       |  +--ro outer-packet-size?   uint16
       +--ro (tunnel-rate)?
       |  +--:(l2-bitrate)
       |  |  +--ro l2-bitrate?     uint64
       |  +--:(l3-bitrate)
       |     +--ro l3-bitrate?     uint64
       +--ro dont-fragment?        boolean
```

User Provided Config
(same as IKE, under spd-entry grouping)

Operational (Actual) Config
(diff from IKE, now under SAD entry)

Statistics augment **`ipsec-ike`** (all-new)

```
augment /nsfike:ipsec-ike/nsfike:conn-entry/nsfike:child-sa-info:
   +--ro ipsec-stats {ipsec-stats}?
   |  +--ro tx-packets?         uint64
   |  +--ro tx-octets?          uint64
   |  +--ro tx-drop-packets?    uint64
   |  +--ro rx-packets?         uint64
   |  +--ro rx-octets?          uint64
   |  +--ro rx-drop-packets?    uint64
   +--ro iptfs-stats {iptfs-stats}?
      +--ro tx-inner-packets?               uint64
      +--ro tx-inner-octets?                uint64
      +--ro tx-extra-pad-packets?           uint64
      +--ro tx-extra-pad-octets?            uint64
      +--ro tx-all-pad-packets?             uint64
      +--ro tx-all-pad-octets?              uint64
      +--ro rx-inner-packets?               uint64
      +--ro rx-inner-octets?                uint64
      +--ro rx-extra-pad-packets?           uint64
      +--ro rx-extra-pad-octets?            uint64
      +--ro rx-all-pad-packets?             uint64
      +--ro rx-all-pad-octets?              uint64
      +--ro rx-errored-packets?             uint64
      +--ro rx-missed-packets?              uint64
      +--ro rx-incomplete-inner-packets?    uint64
```

IPsec Statistics

IP-TFS Statistics

Statistics augment `ipsec-ikeless` (all-new)

```
augment /nsfikels:ipsec-ikeless/nsfikels:sad/nsfikels:sad-entry:
   +--rw ipsec-stats {ipsec-stats}?
   |  +--ro tx-packets?         uint64
   |  +--ro tx-octets?          uint64
   |  +--ro tx-drop-packets?    uint64
   |  +--ro rx-packets?         uint64
   |  +--ro rx-octets?          uint64
   |  +--ro rx-drop-packets?    uint64
   +--rw iptfs-stats {iptfs-stats}?
      +--ro tx-inner-packets?               uint64
      +--ro tx-inner-octets?                uint64
      +--ro tx-extra-pad-packets?           uint64
      +--ro tx-extra-pad-octets?            uint64
      +--ro tx-all-pad-packets?             uint64
      +--ro tx-all-pad-octets?              uint64
      +--ro rx-inner-packets?               uint64
      +--ro rx-inner-octets?                uint64
      +--ro rx-extra-pad-packets?           uint64
      +--ro rx-extra-pad-octets?            uint64
      +--ro rx-all-pad-packets?             uint64
      +--ro rx-all-pad-octets?              uint64
      +--ro rx-errored-packets?             uint64
      +--ro rx-missed-packets?              uint64
      +--ro rx-incomplete-inner-packets?    uint64
```

IPsec Statistics

IP-TFS Statistics

IP –TFS Tunnel Mode Packets - Summary