Donald Fedyk
Christian Hopps
LabN Consulting, LLC

YANG Model for IP Traffic Flow Security

IETF 108 – “draft-fedyk-ipsecme-yang-iptfs-00”

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

IP-TFS Config augment `ipsec-ike`

```
module: ietf-ipsecme-iptfs
  augment /ike:ipsec-ike/ike:conn-entry
          /ike:spd/ike:spd-entry
          /ike:ipsec-policy-config/ike:processing-info
          /ike: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
```

User Provided Config

```
  augment /ike:ipsec-ike/ike:conn-entry
          /ike: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
```

Operational (Actual) Config

IP-TFS Config augment ipsec-ikeless

```
augment /ikeless:ipsec-ikeless
        /ikeless:spd/ikeless:spd-entry
        /ikeless:ipsec-policy-config/ikeless:processing-info
        /ikeless: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
```

User Provided Config

(same as IKE, under spd-entry grouping)

```
augment /ikeless:ipsec-ikeless
        /ikeless:sad/ikeless: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
```

Operational (Actual) Config

(diff from IKE, now under SAD entry)

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

$$\text{IP-TFS Protocol Overhead} = \text{Outer Packet Octets} - \text{Inner Packet Octets} - \text{Pad Octets}$$

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

```
augment /ike:ipsec-ike/ike:conn-entry/ike:child-sa-info:
   +--ro tx-packets?                    uint64 {ipsec-stats}?
   +--ro tx-octets?                     uint64 {ipsec-stats}?
   +--ro tx-drop-packets?               uint64 {ipsec-stats}?
   +--ro rx-packets?                    uint64 {ipsec-stats}?
   +--ro rx-octets?                     uint64 {ipsec-stats}?
   +--ro rx-drop-packets?               uint64 {ipsec-stats}?
   +--rw rx-dropped-packet-detail {ipsec-stats}?
   |  +--ro sa-non-exist?   uint64
   |  +--ro queue-full?     uint64
   |  +--ro auth-failure?   uint64
   |  +--ro malform?        uint64
   |  +--ro replay?         uint64
   |  +--ro large-packet?   uint64
   |  +--ro invalid-sa?     uint64
   |  +--ro policy-deny?    uint64
   |  +--ro other-reason?   uint64
   +--ro tx-inner-packets?              uint64 {iptfs-stats}?
   +--ro tx-inner-octets?               uint64 {iptfs-stats}?
   +--ro tx-extra-pad-packets?          uint64 {iptfs-stats}?
   +--ro tx-extra-pad-octets?           uint64 {iptfs-stats}?
   +--ro tx-all-pad-packets?            uint64 {iptfs-stats}?
   +--ro tx-all-pad-octets?             uint64 {iptfs-stats}?
   +--ro rx-inner-packets?              uint64 {iptfs-stats}?
   +--ro rx-inner-octets?               uint64 {iptfs-stats}?
   +--ro rx-extra-pad-packets?          uint64 {iptfs-stats}?
   +--ro rx-extra-pad-octets?           uint64 {iptfs-stats}?
   +--ro rx-all-pad-packets?            uint64 {iptfs-stats}?
   +--ro rx-all-pad-octets?             uint64 {iptfs-stats}?
   +--ro rx-errored-packets?            uint64 {iptfs-stats}?
   +--ro rx-missed-packets?             uint64 {iptfs-stats}?
   +--ro rx-incomplete-inner-packets?   uint64 {iptfs-stats}?
```

IPsec Statistics

IP-TFS Statistics

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

```
augment /ikeless:ipsec-ikeless/ikeless:sad/ikeless:sad-entry:

   +--ro tx-packets?                  uint64 {ipsec-stats}?
   +--ro tx-octets?                   uint64 {ipsec-stats}?
   +--ro tx-drop-packets?             uint64 {ipsec-stats}?
   +--ro rx-packets?                  uint64 {ipsec-stats}?
   +--ro rx-octets?                   uint64 {ipsec-stats}?
   +--ro rx-drop-packets?             uint64 {ipsec-stats}?
   +--rw rx-dropped-packet-detail {ipsec-stats}?
   |  +--ro sa-non-exist?   uint64
   |  +--ro queue-full?     uint64
   |  +--ro auth-failure?   uint64
   |  +--ro malform?        uint64
   |  +--ro replay?         uint64
   |  +--ro large-packet?   uint64
   |  +--ro invalid-sa?     uint64
   |  +--ro policy-deny?    uint64
   |  +--ro other-reason?   uint64
   +--ro tx-inner-packets?            uint64 {iptfs-stats}?
   +--ro tx-inner-octets?             uint64 {iptfs-stats}?
   +--ro tx-extra-pad-packets?        uint64 {iptfs-stats}?
   +--ro tx-extra-pad-octets?         uint64 {iptfs-stats}?
   +--ro tx-all-pad-packets?          uint64 {iptfs-stats}?
   +--ro tx-all-pad-octets?           uint64 {iptfs-stats}?
   +--ro rx-inner-packets?            uint64 {iptfs-stats}?
   +--ro rx-inner-octets?             uint64 {iptfs-stats}?
   +--ro rx-extra-pad-packets?        uint64 {iptfs-stats}?
   +--ro rx-extra-pad-octets?         uint64 {iptfs-stats}?
   +--ro rx-all-pad-packets?          uint64 {iptfs-stats}?
   +--ro rx-all-pad-octets?           uint64 {iptfs-stats}?
   +--ro rx-errored-packets?          uint64 {iptfs-stats}?
   +--ro rx-missed-packets?           uint64 {iptfs-stats}?
   +--ro rx-incomplete-inner-packets? uint64 {iptfs-stats}?
```

IPsec Statistics

IP-TFS Statistics

Existing IPsec YANG

- ietf-i2nsf-sdn-ipsec-flow-protection
  - Only active/published IPsec YANG model
  - https://tools.ietf.org/html/draft-ietf-i2nsf-sdn-ipsec-flow-protection-07
  - Submitted to IESG for Publication
  - Defines
    - ietf-ipsec-common@2019-08-05.yang
    - ietf-ipsec-ike@2019-08-05.yang
    - ietf-ipsec-ikeless@2019-08-05.yang
  - IP-TFS YANG augments this model
- Also Expired: draft ietf-tran-ipsecme-yang-01
  - https://tools.ietf.org/html/draft-tran-ipsecme-yang-01

Open Issue – SDN IPsec model

- The SDN model provides for an IKE and IKE-less operation
- IKE module intentionally missing a Security Association Database
  - Reason given: centralized controler (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) missing Basic IPsec counters
  - Missing from IKE-less SAD entries
  - Also missing under IKE `child-sa-info`

Open Issue – SDN IPsec model (cont)

- Could easily be modified to allow for more general use.
- Move SAD into common model prior to publishing
  - IKE could then refer to the CHILD_SA in child-sa-info
  - Would provide for missing SA info (transforms, etc)
- Move SPD into common model prior to publishing
  - IKE still utilizes SPDs
  - SPDs are operational data that the user may wish to query
- Otherwise, probably need to rename modules to add "sdn" to their names

SDN IPsec proposed changes (ikeless/common)

```
module: ietf-ipsec-ikeless

  +--rw ipsec-ikeless
     +--rw spd
     |  +--rw spd-entry* [name]
     |     +--rw name
     |     +--rw direction?
     |     +--rw reqid?
     |     ...
     +--rw sad
        +--rw sad-entry* [name]
           +--rw name
           +--rw reqid?
           +--rw ipsec-sa-config
           ...
  notifications:
    +---n sadb-acquire
    +---n sadb-expire
    +---n sadb-seq-overflow
    +---n sadb-bad-spi
```

```
module: ietf-ipsec-common

  +--rw ipsec-common
     +--rw spd
     |  +--rw spd-entry* [name]
     |     +--rw name
     |     +--rw direction?
     |     +--rw reqid?
     |     ...
     +--rw sad
        +--rw sad-entry* [name]
           +--rw name
           +--rw reqid?
           +--rw ipsec-sa-config
           ...
```

SDN IPsec proposed changes (IKE)

```
module: ietf-ipsec-ike

  +--rw ipsec-ike
     +--rw pad
     |  +--rw pad-entry* [name]
     |     +--rw name
        ...
     +--rw conn-entry* [name]
     |  +--rw name
     |  +--rw local
     |  |  +--rw local-pad-entry-name?
     |  +--rw remote
     |  |  +--rw remote-pad-entry-name?
        ...
     |  +--rw spd
     |  |  +--rw spd-entry* [name]
     |  |     +--rw name
     |  |     +--rw ipsec-policy-config
     |  |        +--rw anti-replay-window?
     |  |        +--rw traffic-selector
                 ...
     |  +--rw child-sa-info
     |  |  +--rw pfs-groups*
     |  |  +--rw child-sa-lifetime-soft
     |  |  +--rw child-sa-lifetime-hard
```

```
module: ietf-ipsec-ike

  +--rw ipsec-ike
     +--rw pad
     |  +--rw pad-entry* [name]
     |     +--rw name
        ...
     +--rw conn-entry* [name]
     |  +--rw name
     |  +--rw local
     |  |  +--rw local-pad-entry-name?
     |  +--rw remote
     |  |  +--rw remote-pad-entry-name?
        ...
     |  +--rw spd
     |  |  +--rw spd-entry* [leaf-list references to common spd]
     |  +--rw child-sa-info
     |  |  +--rw pfs-groups*                     pfs-group
     |  |  +--sad-entry [reference to common sad entry]
```

IP-TFS YANG post changes

- IP-TFS config augments ipsec-common SPD entry
  - Previously under ike:conn-entry/ike:spd-entry
  - Previously under ikeless:spd/ikeless:spd-entry

- IP-TFS oper-config augments ipsec-common SAD entry
  - Previously under ike:conn-entry/ike:child-sa-info
  - Previously under ikeless:sad/ikeless:sad-entry

- IP-TFS oper-statistics augments ipsec-common SAD entry
  - Previously not available under ike
  - Previously under ikeless:sad/ikeless:sad-entry

- IP-TFS oper-statistics augment child-sa-info
  - For aggregate statistics
  - Same as before

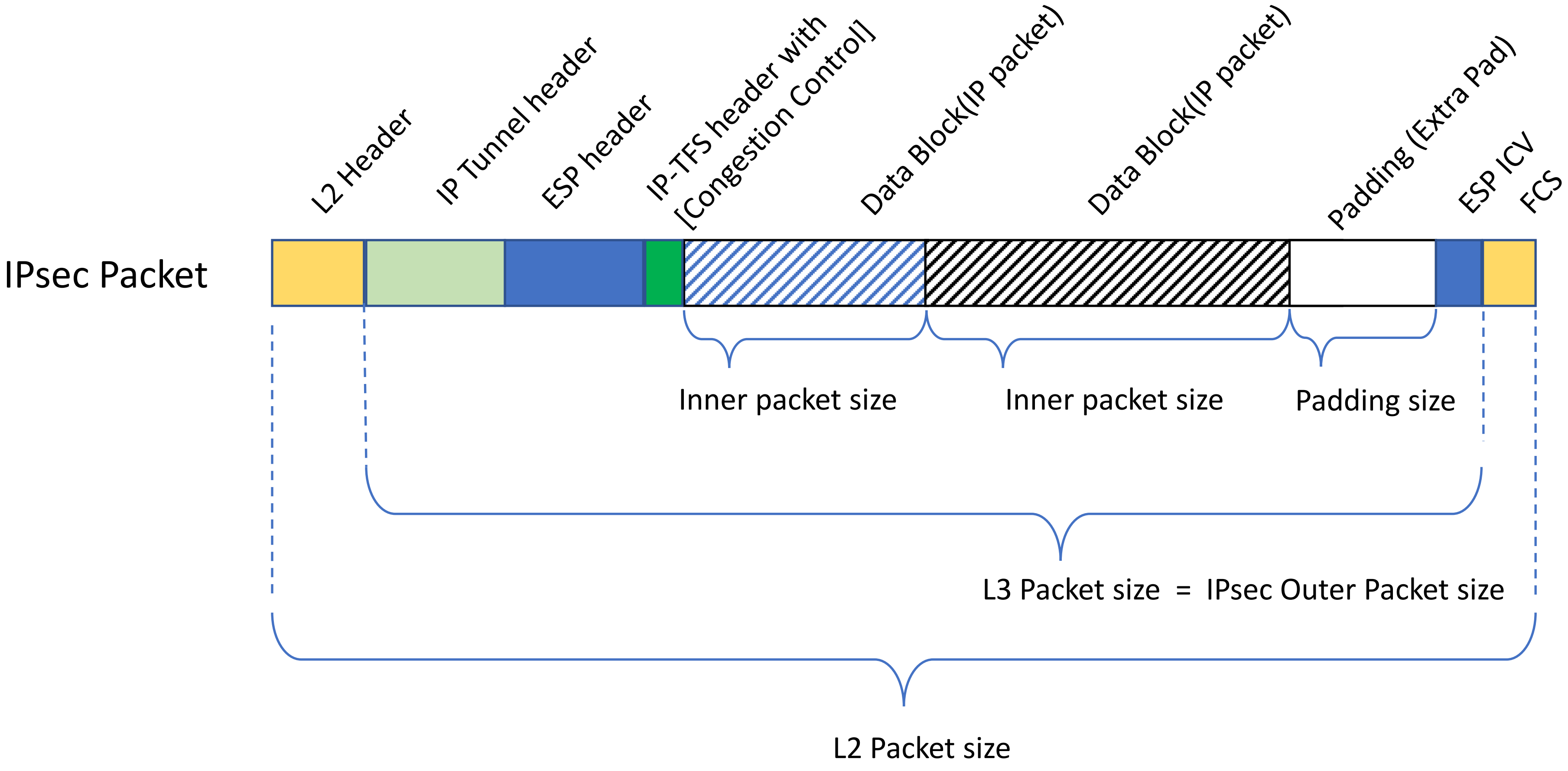
Comments / Questions?

Backup Slides

Context: IPsec Traffic Flow Security (IP-TFS)

- Provide Configuration Control and Statistics for IP-TFS
  - https://tools.ietf.org/html/draft-ietf-ipsecme-iptfs-01
- TFS in a Nutshell
  - Uses Packet Confidentiality of Tunnel Mode
  - Adds fixed size packets with aggregation and padding
  - Adds fixed transmission interval
  - Can be run with Congestion control
  - Provides Aggregation of inner packets
  - Utilizes Fragmentation of inner packets for efficiency
  - Tunnel Ingress controls packet format and frequency
    - A Self describing data block format allows sender traffic pattern flexibility

IP –TFS Tunnel Mode Packets - Summary


L2 Header
IP Tunnel header
ESP header
IP-TFS header with
[Congestion Control]
Data Block(IP packet)
Data Block(IP packet)
Padding (Extra Pad)
ESP ICV
FCS
IPsec Packet
Inner packet size
Inner packet size
Padding size
L3 Packet size = IPsec Outer Packet size
L2 Packet size