

Donald Fedyk
Christian Hopps
LabN Consulting, LLC

YANG Model for IP Traffic Flow Security

IETF 110 – “draft-fedyk-ipsecme-yang-iptfs-02”

Changes since IETF110

- Updates based on comments received during adoption call
 - Reorganized statistics (separated inner and outer stats)
 - Added max-aggregation-time
 - Tracked name changes from I2NSF YANG model (per IESG publication review)
 - Changes included in draft-fedyk-ipsecme-yang-iptfs-02
- Adopted by WG
 - Republishing as draft-ietf-ipsecme-yang-iptfs-00

Current Tree (ike version shown)

```
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-discovery?  boolean
  |   +---rw outer-packet-size?      uint16
  +---rw (tunnel-rate)?
  |   +---:(12-fixed-rate)
  |   |   +---rw 12-fixed-rate?      uint64
  |   +---:(13-fixed-rate)
  |   |   +---rw 13-fixed-rate?      uint64
  +---rw dont-fragment?           boolean
  +---rw max-aggregation-time?    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)?
  |   +---:(12-fixed-rate)
  |   |   +---ro 12-fixed-rate?      uint64
  |   +---:(13-fixed-rate)
  |   |   +---ro 13-fixed-rate?      uint64
  +---ro dont-fragment?           boolean
```

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

Next Steps

- Track changes in the base IPsec specification
- Solicit feedback from the WG

Donald Fedyk
Eric Kinzie
LabN Consulting, LLC

Definitions of Managed Objects for IP Traffic Flow Security

IETF 110 – “draft-fedyk-ipsecme-mib-iptfs-00”

Objective: Provide a read only SNMP MIB

- Some operators still require read-only SNMP support
- Mechanically derived from the YANG model

```
leaf l2-fixed-rate {  
  type uint64;  
  description  
    "Target bandwidth/bit rate in bps for iptfs tunnel. This  
    fixed rate is the nominal timing for the fixed size packet.  
    If congestion control is enabled the rate may be adjusted  
    down (or up if unset).";  
  reference  
    "draft-ietf-ipsecme-iptfs section 4.1";  
}
```



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

MIB Tree

```

---- iptfsMIB(1.3.6.1.3.500)
+---- iptfsMIBObjects(1)
+---- iptfsGroup(1)
+---- iptfsConfigTable(1)
+---- iptfsConfigTableEntry(1) [iptfsConfigsSaIndex]
+---- iptfsConfigSaIndex(1) Integer32
+--r- congestionControl(2) TruthValue
+--r- usePathMtu(3) TruthValue
+--r- outerPacketSize(4) UnsignedShort
+--r- l2FixedRate(5) Counter64
+--r- l3FixedRate(6) Counter64
+--r- dontFragment(7) TruthValue
+--r- maxAggregationTime(8) NanoSeconds
+---- ipsecStatsGroup(2)
+---- ipsecStatsTable(1)
+---- ipsecStatsTableEntry(1) [ipsecSaIndex]
+---- ipsecSaIndex(1) Integer32
+--r- txPackets(2) Counter64
+--r- txOctets(3) Counter64
+--r- txDropPackets(4) Counter64
+--r- rxPackets(5) Counter64
+--r- rxOctets(6) Counter64
+--r- rxDropPackets(7) Counter64

```

```

+---- iptfsInnerStatsGroup(3)
+---- iptfsInnerStatsTable(1)
+---- iptfsInnerStatsTableEntry(1) [iptfsInnerSaIndex]
+---- iptfsInnerSaIndex(1) Integer32
+--r- txInnerPackets(2) Counter64
+--r- txInnerOctets(3) Counter64
+--r- rxInnerPackets(4) Counter64
+--r- rxInnerOctets(5) Counter64
+--r- rxIncompleteInnerPackets(6) Counter64
+---- iptfsOuterStatsGroup(4)
+---- iptfsOuterStatsTable(1)
+---- iptfsOuterStatsTableEntry(1) [iptfsSaIndex]
+---- iptfsSaIndex(1) Integer32
+--r- txExtraPadPackets(2) Counter64
+--r- txExtraPadOctets(3) Counter64
+--r- txAllPadPackets(4) Counter64
+--r- txAllPadOctets(5) Counter64
+--r- rxExtraPadPackets(6) Counter64
+--r- rxExtraPadOctets(7) Counter64
+--r- rxAllPadPackets(8) Counter64
+--r- rxAllPadOctets(9) Counter64
+--r- rxErroredPackets(10) Counter64
+--r- rxMissedPackets(11) Counter64
+---- iptfsMIBConformance(2)
+---- iptfsMIBConformances(1)
| +---- iptfsMIBCompliance(1)
+---- iptfsMIBGroups(2)
+---- iptfsMIBConfGroup(1)
+---- ipsecStatsConfGroup(2)
+---- iptfsInnerStatsConfGroup(3)
+---- iptfsOuterStatsConfGroup(4)

```

Next Steps

- Ready for WG adoption?

Comments / Questions?